

基于三维超混沌系统的彩色图像加密算法

赵怀勋, 程 甲

(武警工程学院 通信工程系, 陕西 西安 710086)

摘 要: 针对彩色图像的存储特性, 为了改进彩色图像加密算法的安全性和效率, 提出了一种基于三维超混沌系统的彩色图像加密算法. 该算法利用改进的三维超混沌系统产生混沌序列, 采用复合加密算法实现彩色图像在空域上的加密. 使用 MATLAB7.0 进行仿真实验. 理论分析和实验表明, 该算法具有良好的保密性和加密效果. 若进一步降低运算量, 该算法可对诸如军事卫星图片、商业机密图纸、远程私人病历等需要保密通信的场合有广泛的应用前景.

关键词: 三维超混沌系统; 彩色图像加密; 混沌序列

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)02-0072-03

Color Image Encryption Algorithm Based on Three-Dimension Chaotic System

ZHAO Huai-xun, CHENG Jia

(Department of Communicate Engineering, Armed Police Engineering College, Xi'an 710086, China)

Abstract: In view of the storage characteristic of color images, in order to extend the effect and security of image encryption algorithm. A color image encryption algorithm based on the three-dimension chaotic system was proposed. Firstly, the chaotic sequence were adopted by the three-dimension chaotic system. Then a color image was encrypted in space domain by using composite encryption algorithm. Using MATLAB7.0 carried out simulation. Theoretical analysis and simulated experiment show that, algorithm guarantees the security of the encryption effectively and excellent effect of encryption. If reduces the computation, the algorithm can be used widely in military satellite images, trade secret drawings, long-range private medical that wanted to be kept confidential communications.

Key words: three-dimension chaotic system; color image encryption; chaos sequence

1 引言

随着网络技术的飞速发展和多媒体数字产品的广泛应用, 确保多媒体信息在传播和使用过程中的安全是迫切需要解决的问题. 数字图像具有数据量大、数据相关度高等特点, 用传统的加密方式对图像加密存在效率低的缺点. 近年来兴起的新型混沌加密方法为图像加密提供了一种新的有效途径, 已成为研究热点^[1-3].

对彩色图像加密大多都采用基于 (k, n) 秘密共

享的加密算法^[4-5] ($1 \leq k \leq n$), 这种算法的优点是个别子图像的泄漏不会引起原始图像的泄漏, 个别子图像的丢失也不会影响原始图像的恢复. 该算法简单直观、安全性好, 具有较好的抗干扰性. 但是, 这种算法存在一个很严重的缺点, 就是会使图像数据量发生膨胀, 这在图像数据本来就很大的情况下给图像的网络传输带来困难, 限制了这种加密算法在实际中的应用^[6].

文中提出一种基于三维超混沌系统^[7]的彩色图像加密算法, 既能扩大密钥空间, 提高加密系统的抗破译强度, 又能弥补基于秘密共享加密算法的缺陷.

2 三维超混沌系统的彩色图像加密算法设计

一幅 24 位的真彩色图像由 RGB 三原色组成, 可以表示为 $M \times N \times 3$ 三维数组的形式, 且相邻像素的三原色值在空间域上具有很强的相关性. 所以, 基于三维超混沌系统的彩色图像加密算法就是利用混沌系统产生的密钥序列分别作用于 RGB 三原色, 扰乱三原色在空间域中的相关性, 使原彩色图像变成一幅杂乱无章的图像, 无法识别, 从而达到良好的加密效果.

2.1 密钥的产生

一维混沌加密算法利用混沌序列的良好复杂性、伪随机性和对初值的敏感特性, 具有较好的加密性能, 但与其他方法相比, 最大的缺点就是密钥空间太小. 为此, 需要一种基于高维超混沌系统的图像加密方法来扩大密钥空间, 提高加密系统的抗破译强度. 因此, 采用三维超混沌系统, 其形式为

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

式中, 参数 a, b, c 的典型值分别为 $a = 35, b = 3, c \in [20, 28.4]$ 时, 系统进入混沌状态, 其混沌吸引子如图 1 所示.

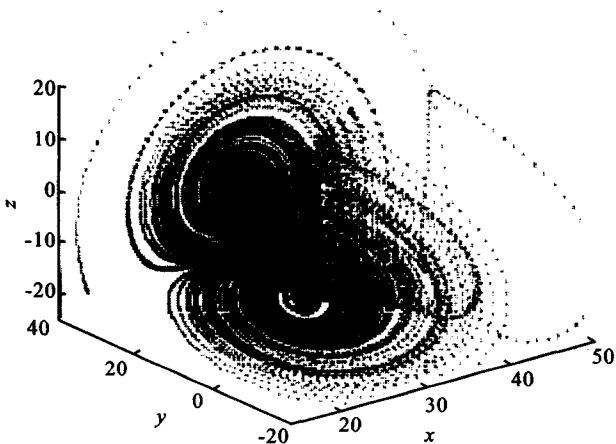


图1 三维超混沌吸引子

但该系统输出的实值混沌序列有一些固有缺陷: x, y, z 的值域各不相同, 不利于批处理; x, y, z 局部取值呈现单调性, 易受线性预测攻击; x, y, z 自相关特性非理想的 δ 函数, 互相关特性非理想的零特性, 难以保证不可预测性, 而且系统多输出特性也得不到充分利用. 为此, 文献[8]中提出了一种对此混沌序列的优化方法, 构建新的数学模型为

$$\begin{cases} x = 10^m x - \text{round}(10^m x) \\ y = 10^m y - \text{round}(10^m y) \\ z = 10^m z - \text{round}(10^m z) \end{cases} \quad (2)$$

式中, x, y, z 为优化后的实值混沌序列; m 为控制参数, 通过它可以提高序列取值的不规则性; $\text{round}()$ 为取靠近零的整数函数. 文献[8]中经过实验, 证明此优化序列具有良好的混沌特性、较理想的函数自相关特性和近似为 0 的互相关特性.

另外, 为了增强抗破译强度还将扩散函数的思想应用到密钥中, 将密文中的像素值嵌入到密钥发生器中, 具体形式为

$$\begin{cases} x = \text{fabs}(x) - \text{round}(\text{fabs}(x)) + (k_R \oplus (256 * f_{k+1}) / 256) \bmod 1 \\ y = \text{fabs}(y) - \text{round}(\text{fabs}(y)) + (k_G \oplus (256 * f_{k+1}) / 256) \bmod 1 \\ z = \text{fabs}(z) - \text{round}(\text{fabs}(z)) + (k_B \oplus (256 * f_{k+1}) / 256) \bmod 1 \end{cases} \quad (3)$$

式中, $\text{fabs}(x)$ 是取 x 的绝对值, $\text{round}()$ 为取 $\text{fabs}(x)$ 靠近零的整数. k_R, k_G 和 k_B 分别表示密文中一个像素的 R, G 和 B 分量值, f_{k+1} 是常用的 Logistic 映射所产生的混沌序列值.

由上式可见, 通过将密文中的像素分量 R, G 和 B 值嵌入到密钥发生器中, 可以增强扩散函数的影响, 将密文中每一位像素的影响扩散到整个密文中.

2.2 加密算法

对一幅大小为 $M \times N \times 3$ 的 24 位真彩色图像进行加密处理, 具体过程如下:

步骤一: 输入原始图像 $I_{M \times N}$, 混沌系统初始值 x_0, y_0 和 z_0 ;

步骤二: 利用式(1)和式(2)表示的三维混沌系统生成混沌序列 $\{x_k, y_k, z_k, k = 1, 2, 3, \dots\}$. 取该序列的某一连续片断(如 $1000 < k \leq 1000 + M \times N$), 利用式(4)生成第一个加密密文 k'_R, k'_G, k'_B (此时式(4)中的 $k'_{R-1}, k'_{B-1}, k'_{G-1}$ 均取值为 0);

步骤三: 将 k'_R, k'_G, k'_B 代入式(3)中生成最终用来加密图像的混沌序列值 $x_t, y_t, z_t (t = 2, 3, 4, \dots)$;

步骤四: 利用生成的混沌序列 $\{x_t, y_t, z_t, t = 2, 3, 4, \dots\}$ 来加密原始图像 $I_{M \times N}$, 具体加密方法如式(4)所示.

$$\begin{cases} k'_R = ((k_R + (k'_{R-1})^2 + 256 * x) \bmod 256) \oplus \\ (256 * f_{k+1}) \oplus k'_{G-1} \oplus k'_{B-1} \\ k'_G = ((k_G + (k'_{G-1})^2 + 256 * y) \bmod 256) \oplus \\ (256 * f_{k+1}) \oplus k'_{G-1} \oplus k'_{B-1} \\ K'_B = ((k_B + (k'_{B-1})^2 + 256 * z) \bmod 256) \oplus \\ (256 * f_{k+1}) \oplus k'_{G-1} \oplus k'_{R-1} \end{cases} \quad (4)$$

式中, k_R, k_G, k_B 分别表示待加密像素点的 R, G, B 分量值, k'_R, k'_G, k'_B 分别表示已加密像素点的 R, G, B 分量值, $k'_{R-1}, k'_{B-1}, k'_{G-1}$ 分别表示前一个加密像素点的 R, G, B 分量值;

步骤五:从第二个到最后一个像素点重复步骤四到步骤五的操作,直至所有像素点完成加密操作;

步骤六:输出加密图像 $I'_{M \times N}$.

2.3 实验结果及分析

在 Matlab7.0 仿真环境下对一幅 24 位真彩色图像进行加密和解密实验,设置参数分别为 $a = 35$, $b = 3$, $c = 28$,设置系统初始值分别为 $x_0 = 0.258$, $y_0 = 0.368$, $z_0 = 0.568$,图像加密效果如图 2 所示.

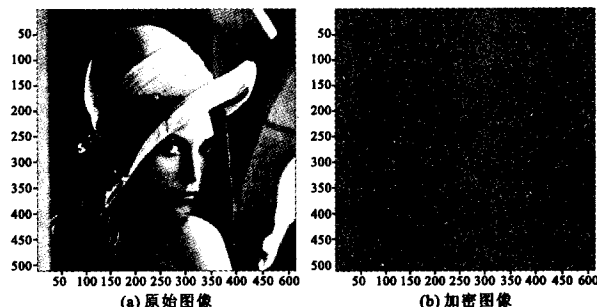


图 2 加密效果图

分析上述实验结果,文中加密算法的特点如下:

(1)从实验结果可以看出,应用本算法对图像进行加密处理后,原始图像已失去它本来面目,变得杂乱无章,无法辨认,该算法有很好的加密效果.

(2)所采用的三维超混沌映射对初始值 x_0, y_0 和 z_0 具有很强的敏感依赖性,三者只要其中一个有微小的变化就无法得到正确的解密结果.因此,采用本算法进行图像加密是非常安全的,且其密钥空间大,经分析可达 1054,可以有效的抵抗恶意攻击.

(3)由于采用的算法是在空域对图像数据进行整数运算处理,处理操作(异或和加法运算)比较简单,所以加密效率很高.

3 结束语

基于三维超混沌系统的彩色图像加密算法是在传统混沌加密算法的基础上,将密文中的像素值嵌入到密钥发生器,并在加密算法中应用了密文反馈算法.分析和仿真实验表明,该算法具有较高的加密效率,可以有效地提高加密图像的保密性和安全性.若进一步降低运算量,该算法可对诸如军事卫星图片、商业机密图纸、远程私人病历等需要保密通信的场合有广泛的应用前景.

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] Longm, Peng F, Qiu S S, et al. Implementation of a new chaotic encryption system and synchronization[J]. Journal of Systems Engineering and Electronics, 2006, 17(1): 43 - 47.
- [3] Gao H J, Zhang Y S, Liang S Y, et al. A new chaotic algorithm for image encryption[J]. Chaos, Solitons and Fractals, 2006, 29(2): 393 - 399.
- [4] Lukac R, Plataniotis K N. Colour image secret sharing [J]. IEEE Electron. Lett. 2004, 40(9): 529 - 530.
- [5] Lukac R, Plataniotis K N. Bit - level based secret sharing for image encryption[J]. IEEE Signal Processing Letters, 2004, 38(5): 767 - 772.
- [6] 刘建东. 基于超混沌序列的自适应数字图像隐藏算法 [J]. 微电子学与计算机, 2005, 22(3): 173 - 177.
- [7] Fei Peng, Qiu Shuisheng, Min Long. An image encryption algorithm based on mixed chaotic systems and external keys [C]// 2005 International Conference on Communications. China: Guangzhou, Circuits and Systems - Processings, 2005: 1135 - 1139.
- [8] Wang Ying, Zheng Deling, Ju Lei, et al. The spatial - domain encryption of digital images based on high - dimension chaotic system[C]// Proc of the 2004 IEEE Conference on Cybernetics and Intelligent Systems. Singapore, Haerbin, 2004.

作者简介:

赵怀勋 男,硕士,教授.研究方向为信息安全.

程 甲 男,硕士.研究方向为图像加密.