

一种新的图像加密算法研究与应用

盛苏英¹, 吴新华²

(1 南通大学 电气工程学院, 江苏 南通 226019; 2 南通纺织职业技术学院 现教中心, 江苏 南通 226007)

摘 要: 提出了一种新的混沌彩色图像加密算法. 首先由 Logistic 和 Cubic-Henon 复合混沌映射生成混沌序列, 再结合像素值替代和图像位置置乱方法对彩色图像进行加密, 并利用“一幅图像一次密钥”的密钥同步方案, 实现了一个基于混沌的图像保密通信系统. 该算法具有一定的有效性和良好的加密性能.

关键词: 混沌序列; 彩色图像加密; 密钥同步

中图分类号: TP309.7; TP391

文献标识码: A

文章编号: 1000-7180(2011)02-0124-05

Study and Application of a New Image Encryption Algorithm

SHENG Su-ying¹, WU Xin-hua²

(1 School of Electrical Engineering, Nantong University, Nantong 226019, China;

2 Modern Education Technology Center, Nantong Textile Vocational Technology College, Nantong 226007, China)

Abstract: A new chaotic color image encryption algorithm is presented with the perfect properties of chaotic sequences. At first, the chaotic sequences are generated of Logistic and Cubic-Henon compound chaotic maps. Then the color image is encrypted combining the methods of pixel value substituting and position shuffling. And the image secure communication system based on chaos is designed and implemented, using key synchronization scheme of “one image with one key”. The results of system testing show that the algorithm is valid and has good performance.

Key words: chaotic sequences; color image encryption; key synchronization

1 引言

随着数字图像处理和多媒体通信技术的飞速发展, 数字图像通信现已成为人类进行信息交流的重要手段之一. 图像加密是图像安全保护的核心技术, 由于数字图像具有数据量大、数据相关度高等特点, 用传统的加密方式存在诸多问题, 近年来兴起的混沌加密方式为图像加密开辟了一个新的天地.

混沌信号具有隐蔽性、不可预测性和易于产生、复制等特点, 非常适合于图像加密. 1989 年, 英国数学家 Matthews 最早提出混沌加密的思想^[1], 此后人们提出了多种基于混沌的图像加密算法, 主要有基于 Arnold 变换、幻方、Hilbert 曲线等的混沌图像位置置乱^[2-4], 以及基于混沌系统的各种像素值替代

方法^[5-6]. 此外, 人们对混沌图像加密算法的应用展开了一定的研究工作, 用 MATLAB 仿真或 VC 编程初步实现了混沌图像保密通信^[7-8].

文中采用 Logistic 和 Cubic-Henon 复合混沌映射, 提出了一种新型的混沌彩色图像加密算法, 并利用“一幅图像一次密钥”的原则, 研究并实现了一个基于混沌的图像保密通信系统. 此种保密通信方法实用性强, 可以方便地嵌入到其它现有的实时通信软件中, 提高系统的保密性.

2 图像加密算法设计

2.1 算法思想

一幅 24 位真彩色图像由 R、G、B 三基色组成, 可以表示为 $M \times N \times 3$ 三维数组的形式, 三基色的

收稿日期: 2010-01-05; 修回日期: 2010-03-22

基金项目: 国家自然科学基金项目(60474076); 江苏省自然科学基金项目(BK2010275); 南通市应用研究计划项目(K2010017)

像素值 $\in[0,255]$,且相邻像素的三基色值在空间域上具有很强的相关性.文中将一幅彩色图像处理成 $M \times 3N$ 灰度图像,然后利用 Logistic 和 Cubic-Henon 复合混沌映射产生混沌序列,对图像进行像素值替换和以 8×8 块为单位的空域置乱,扰乱相邻像素的相关性,再进行重组,从而使得原图像变成一幅杂乱无章的彩色图像,达到良好的加密效果.

2.2 混沌映射

系统采用的 Logistic 混沌映射形式如下:

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

混沌动力系统的研究工作指出:当 $3.5699456 \dots < \mu \leq 4$, $x_n \in (0,1)$ 时,Logistic 映射工作于混沌状

态,而且 Logistic 映射对参数 μ 具有极度敏感性.

系统采用的 Cubic-Henon 复合混沌映射进行图像位置置乱,其方程如下:

$$\begin{cases} x[k+1] = -3x[k] + 4x^3[k] \\ y[k+1] = 1 + 0.3z[k] - 1.4y^2[k] \\ z[k+1] = y[k] \end{cases} \quad (2)$$

其中, $x[k]$ 是 Cubic 混沌映射的状态, $y[k], z[k]$ 是 Henon 混沌映射的状态.

2.3 加/解密算法

文中提出了一种新型的混沌图像加密算法,系统框图如图1所示.具体加密过程描述如下:

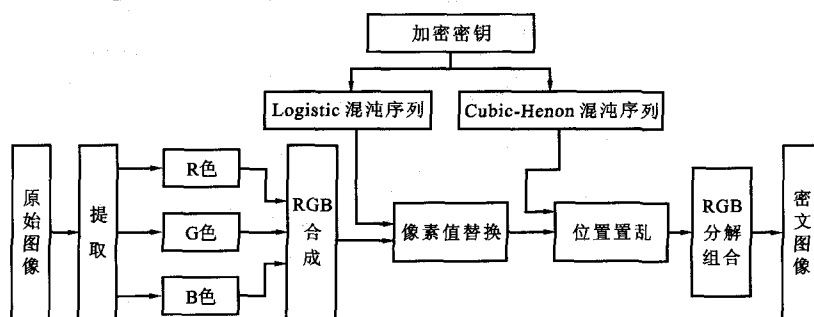


图1 彩色图像加密算法框图

(1) 输入待加密彩色图像,分离彩色图像的RGB三基色分量 $(R_{M \times N}, G_{M \times N}, B_{M \times N})$,将彩色图像的RGB三基色分量进行组合 $[R_{M \times N}, G_{M \times N}, B_{M \times N}]$.

(2) 取 $\mu_1 = 3.95, \mu_2 = 3.97, \mu_3 = 4$,输入初值 xx_0 (令初值为加密密钥),由式(1)分别生成三个混沌序列,将序列中每个元素都扩大至小数点后三位,相加得到 $M \times 3N$ 二维混沌数组 $HW[][]$;再与 $[R_{M \times N}, G_{M \times N}, B_{M \times N}]$ 对应元素相加并求余,得到灰度值替代后加密图像 $RGB_H_{M \times 3N}$.

(3) 给定初值 x_0, y_0, z_0 (同样令初值为加密密钥),由式(2)生成实值混沌序列 x, y ,再将其按由小到大的顺序排列,生成置乱索引二维数组 $PX_{M \times 3N}, PY_{M \times 3N}$,然后以 $PY_{M \times 3N}$ 为行地址置换矩阵,对加密图像 $RGB_H_{M \times 3N}$ 进行行地址变换,以 $PX_{M \times 3N}$ 为列地址置换矩阵,进行列地址变换.

(4) 合成R、G、B三基色,输出密文彩色图像.

解密算法是加密算法的逆运算,恢复出原始彩色图像.

2.4 实验仿真

为了验证文中算法的有效性,对一幅尺寸大小为 $512 \times 512 \times 3$ 的lena图像进行加密,其仿真结果如图2所示.仿真时取加密密钥与解密密钥相同,分

别为 $xx_0 = \hat{xx}_0 = 0.1, x_0 = \hat{x}_0 = 0.655, y_0 = \hat{y}_0 = 0.2, z_0 = \hat{z}_0 = 1.2$.

由图2可知,原始图像经加密后,图像变得杂乱无章、不可识别,而加密图像经正确的密钥解密后又能恢复出原始图像,从而具有一定的有效性和保密性;而且密文图像R、G、B分量的直方图很均匀,完全不同于原始图像R、G、B分量的直方图,可有效地抵抗统计攻击.

3 图像加密算法应用

文中设计并实现了一个混沌图像保密通信系统,具有较强的保密性和较高的实时性,可进行全双工通信.混沌图像保密通信系统的设计思路为图像载入—图像加密—数据发送—数据传输—数据接收—图像解密—图像显示,如图3所示.假设一个客户端往服务器端发送图像信息,首先必须用给定的IP地址和端口号建立连接,加密后通过socket传送密文,接收端接收到密文后进行解密,从而在同步密钥的保证下恢复原始图像信息.考虑到图像保密通信的实际,采用了TCP传输协议,用密钥同步方法保证收发端混沌信号的同步,从而进行图像保密通信.

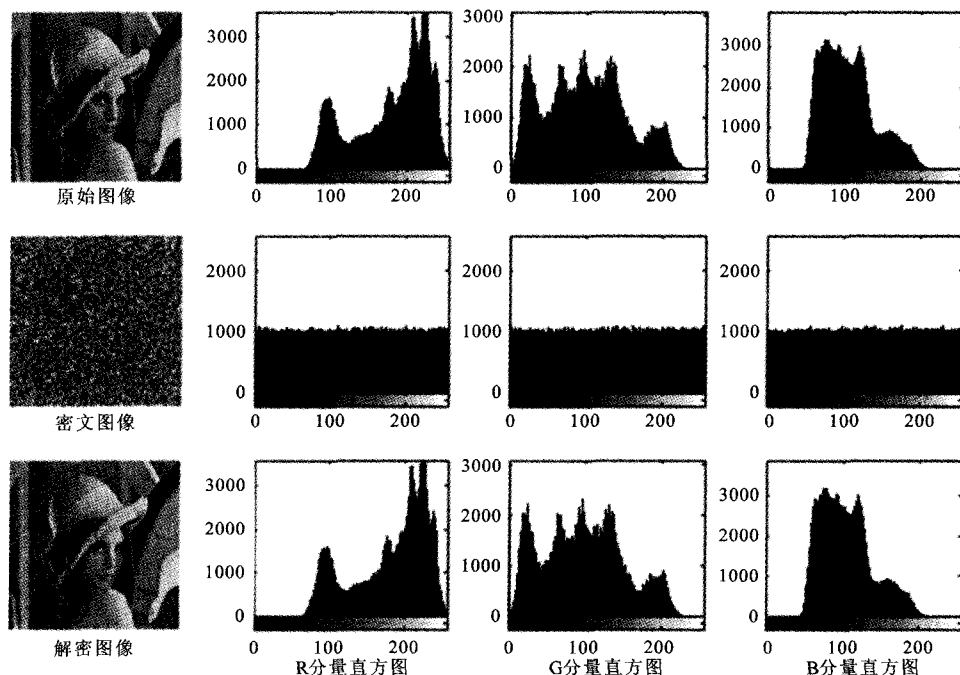


图2 混沌图像加解密仿真图

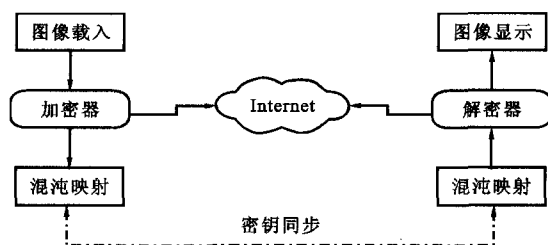


图3 系统框图

对于数字图像保密通信而言,由于系统采用TCP传输协议(可靠传输,能保证混沌加解密对应混沌序列迭代步数一致),如能实现收发端的密钥一致(即密钥同步)时,即可成功恢复出原始图像信息,那如何实现密钥同步呢?

为了保证图像的完整性,同时进一步提高系统的保密性,系统预留原始图像中B基色的最后3个像素点信息(不加密),用于产生同步密钥: $B[M-1][N-3]$ 用于产生密钥 x_0 ; $B[M-1][N-2]$ 用于产生密钥 y_0 ; $B[M-1][N-1]$ 用于产生密钥 z_0 ; B基色3点共同作用产生密钥 xx_0 。前三个为Cubic-Henon复合混沌映射初值,最后一个为Logistic映射初值。

系统预设一个Chebyshev映射 $f(z_0, p)$,方程结构如下,其初值由原始图像预留B基色的最后三个点值提供。

$$z_{n+1} = \cos(p \times \arccos z_n) \quad (3)$$

同步密钥中 x_0 为预设Chebyshev映射迭代 $K1$ 次后所得(参数为 $K1, P1$),表示为:

$$x_0 = f^{K1} \left(\frac{B[M-1][N-3]-128}{128}, P1 \right) + 1$$

同步密钥中 y_0 为预设Chebyshev映射迭代 $K2$ 次后所得(参数为 $K2, P2$),表示为:

$$y_0 = f^{K2} \left(\frac{B[M-1][N-2]-128}{128}, P2 \right) + 1$$

同步密钥中 z_0 为预设Chebyshev映射迭代 $K3$ 次后所得(参数为 $K3, P3$),表示为:

$$z_0 = f^{K3} \left(\frac{B[M-1][N-1]-128}{128}, P3 \right) + 1$$

同步密钥中 xx_0 为预设Chebyshev映射迭代 $K4$ 次后所得(参数为 $K4, P4$),表示为:

$$xx_0 = f^{K4} \left(\frac{B[M-1][N-3]}{3 \times 128} + \frac{B[M-1][N-2]}{3 \times 128} + \frac{B[M-1][N-1]}{3 \times 128} - 1, P4 \right)$$

以上 x_0, y_0, z_0, xx_0 都需处理成满足混沌映射的初值值条件。

参数($K1, P1; K2, P2; K3, P3; K4, P4$)通信双方协定一致,由原始图像预留像素的三基色所产生的混沌加密、解密密钥也一致,即可保证收发端密钥同步。

4 系统测试与性能分析

系统界面类似QQ,操作非常简单。用户点击聊天对象并选择“图像保密通信”后,系统就会为双方

建立 TCP 连接,进入图像通信界面,如图 4 所示. 发送方选择载入的图像文件后,一按“发送图像”按钮,就会将原始图像加密成加密图像后发送;接收方自动弹出“×××有加密图片传输过来,是否接收”的对话框,一旦选择“接收”,就会自行将加密图像按“同步密钥”进行解密,恢复出原始图像信息.

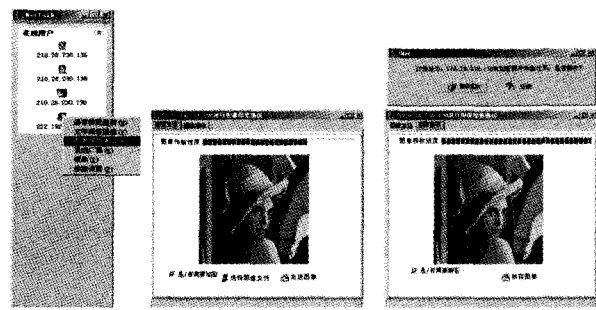


图 4 系统通信界面图

可以看出,建立连接的双方可进行图像保密通信,而在信道中传输的是无法识别的图像信息,因此系统具有较强的保密性,且此系统可扩展为多用户的实时图像保密通信.

4.1 密钥空间和密钥敏感性

在文中提出的加密算法中,Logistic 以及 Cubic-Henon 复合混沌映射的初值作为密钥,即 (x_0, x_0, y_0, z_0) ,其精度达到 10^{-16} ,密钥空间可达 10^{-64} ,可有效地抵抗恶意穷举攻击.

下面首先从密钥失配时的解密图像来定性分析密钥敏感性. 加/解密密钥分别取 $x_0=0.655, \hat{x}_0=0.65500001, y_0=0.2, \hat{y}_0=0.20000001, z_0=1.2, \hat{z}_0=1.20000001, x_0=0.1, x\hat{x}_0=0.10000001$,原始图像见图 2,解密图像如图 5 所示. 可见,尽管加、解密密钥只有微小的偏差,但解密后的图像已看不出任何原始图像的痕迹.

再由图像恢复性能指标 MSE 和 PSNR 来定量描述密钥敏感性. 当解密密钥 $x_0, y_0, z_0, x\hat{x}_0$ 分别以 10^{-2} 的数量级失配时,得到不同的解密图像,测量其与原图像的 MSE 和 PSNR,可得表 1.

表 1 对初值 $x_0, y_0, z_0, x\hat{x}_0$ 微小变化的敏感性测试

x_0				y_0				z_0				$x\hat{x}_0$			
PSNR				PSNR				PSNR				PSNR			
变化	R	G	B	变化	R	G	B	变化	R	G	B	变化	R	G	B
10^{-10}	11.6553	12.3321	13.4092	10^{-10}	11.6913	12.3989	13.4668	10^{-10}	11.6964	12.4038	13.4523	10^{-10}	11.6309	12.3257	13.3900
10^{-8}	11.6458	12.3312	13.4092	10^{-8}	11.6802	12.4024	13.4149	10^{-8}	11.6925	12.4001	13.4555	10^{-8}	11.6305	12.3239	13.3853
10^{-6}	11.6424	12.3301	13.4092	10^{-6}	11.6793	12.3925	13.4126	10^{-6}	11.6834	12.3818	13.4549	10^{-6}	11.6212	12.3206	13.3839
10^{-4}	11.6401	12.3238	13.4092	10^{-4}	11.6735	12.3773	13.4105	10^{-4}	11.6787	12.3800	13.4467	10^{-4}	11.6193	12.3188	13.3809
10^{-2}	11.6359	12.3321	13.4092	10^{-2}	11.6693	12.3709	13.4085	10^{-2}	11.6768	12.3782	13.4456	10^{-2}	11.6105	12.3118	13.3734

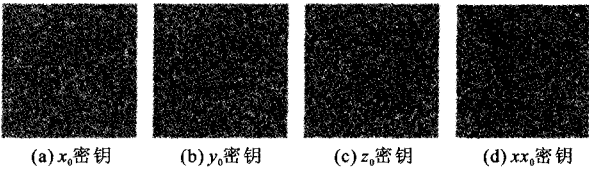


图 5 密钥发生微小变化后的解密效果图

均方误差:

MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I'(i,j) - I(i,j))^2 \tag{4}

峰值信噪比:

PSNR = 10 \lg \left(\frac{f_{\max}^2}{MSE} \right) \tag{5}

可见,密钥的微小变化,可以导致解密图像完全偏离原始图像(通常当 PSNR 值在 28dB 以上时,图像恢复的质量较好),这意味着该算法对密钥具有极大地敏感性.

4.2 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:

cov(x,y) = E((x - E(x))(y - E(y))) \tag{6}

R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}}

其中, x, y 是图像中两相邻像素的像素值, $E(x)$ 是 x 的数学期望, $D(x)$ 是 x 的方差, $cov(x, y)$ 是 x, y 的协方差. 原始图像中相邻像素的相关性是很大的,为了破坏统计攻击,必须是相邻两个像素的相关性降低,相关系数越小说明加密性能越好.

图 6 所示分别为原始图像和加密图像垂直相邻像素点的相关性图,横坐标为 (x, y) 点像素的平均值,纵坐标为 $(x + 1, y)$ 点像素的平均值,原始图像和加密图像垂直相邻像素点的相关性系数分别为 0.9791, 0.0176,具体可见表 2 分析.

现从原始图像和密文图像中任取一行、一列以及对角线上的像素点进行相邻像素相关系数计算,可得如表 2 所示.

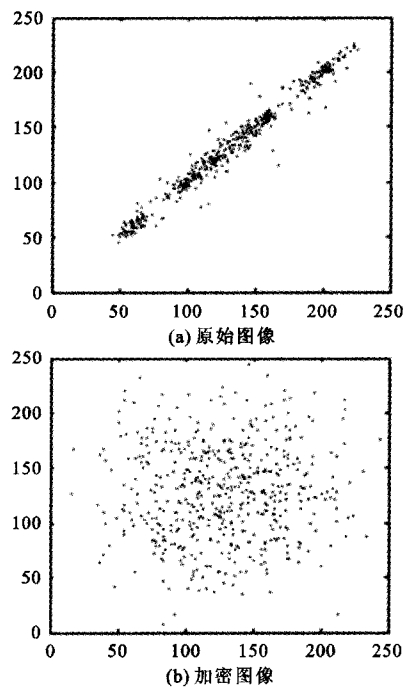


图 6 垂直相邻像素点的相关性图

表 2 相邻像素相关系数

像素关系	原始图像			密文图像		
	R	G	B	R	G	B
水平相邻	0.9798	0.9200	0.8632	0.0423	-0.0308	0.0275
垂直相邻	0.9855	0.9831	0.9686	0.0303	0.0164	0.0062
对角线相邻	0.9635	0.9421	0.8824	-0.0386	0.0252	-0.0159

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能力,加密效果好,因此该算法对统计分析具有更好的安全性.

4.3 抗攻击性测试

密文图像在传输过程中经常会受到噪声污染以及几何失真等影响,图 7 所示为其解密效果.图 7 (a)以 peppers 为例的密文图像受到 10%强度的椒盐噪声污染后的解密图像,其与原图像的相似度为 90.01%;图 7(b)以 pelican 为例的密文图像经约 13.3%不规则裁剪后的解密图像,其与原图像的相似度为 90.08%,可见此算法具有较好的抗噪声、抗裁剪攻击能力.

5 结束语

文中提出了一种新的基于混沌序列的彩色图像加密方法,利用混沌信号的优良特性,结合像素值替

代和图像位置置乱方法,进行图像加密,并利用“一幅图像一次密钥”的密钥同步方案,实现了一个基于混沌的图像保密通信系统.

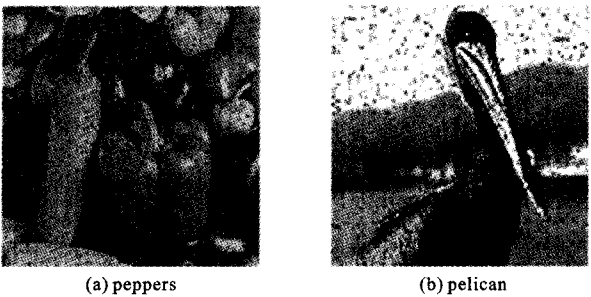


图 7 被攻击后的解密图像

参考文献:

[1] Matthews R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989(1): 29-42.

[2] Chen Guanrong, Mao Yaobao, Chui Charles K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos Solitons & Fractals, 2004, 21(3): 749-761.

[3] 王英,郑德玲,王振龙. 空域彩色图像混沌加密算法[J]. 计算机辅助设计与图形学学报, 2006, 18(16): 877-880.

[4] 赵学峰. 基于混沌映射的数字图像置乱方法[J]. 微电子学与计算机, 2003, 20(8): 136-138.

[5] Fu Chong, Zhang Zhenchuan, Cao yingyu. An improved image encryption algorithm based on chaotic maps[C]// Third international conference on natural computation (ICNC). China: Hainan, 2007: 189-193.

[6] 赵莉,张雪峰,范九伦. 基于混沌序列的数字图像加密算法[J]. 微电子学与计算机, 2007, 24(2): 73-75.

[7] Liao Xiaofeng, Li Xueming. A digital secure image communication scheme based on the chaotic Chebyshev map [J]. International Journal of Communication Systems, 2004, 17(5): 437-445.

[8] 向菲,肖慧娟,丘水生. 基于 CNN 和 DES 的图像保密通信系统设计方案[J]. 华南理工大学学报:自然科学版, 2007, 35 (9): 31-35.

作者简介:

盛苏英 女, (1979-), 硕士, 讲师. 研究方向为混沌同步、混沌保密通信.

吴新华 男, (1980-), 硕士. 研究方向为图像加密.