基于多混沌系统组合图像置乱加密算法研究

洪联系,李传目,卢明玺
(集美大学,福建 厦门 361021)

摘 要:提出一个基于位平面彩色图像Arnold映射置乱和采用Chen系统产生的混沌序列加密算法。首先采用由Logistic系统构造的非线性动力系统产生的混沌序列形成Arnold映射矩阵,在不同的位平面对彩色图像进行置乱,然后用Chen系统产生的混沌序列对置乱后的图像进行加密。该算法实现简单,能够抵御各种攻击,且容易用硬件实现。

关键词:彩色图像加密;Arnold映射;位平面置乱;Chen系统
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)11-0070-04

Study on Composite Image Disorder Encryption Algorithm Based on Multi-Chaotic System

HONG Lian-xi, LI Chuan-mu, LU Ming-xi
(Jimei University, Xiamen 361021, China)

Abstract: Presented an image encryption algorithm based on bit plane color image Arnold disorder approach and the chaotic sequence that is produced by Chen's system. First, the mapped matrixes of Arnold, which their elements are made up of the chaotic sequences that are produced by the Logistic dynamic system, are used for disordering the color image in different bit planes to produce disordered image. Then, the image is encrypted by means of the chaotic sequence that is produced by the Chen's system. The algorithm is very simple, can resist various attacks, and is implemented by means of hardware.

Key words: color image encryption; Arnold map; bit plane disorder; Chen's system

0 引 言

在当前激烈的市场竞争中,技术因素占据着十分重要的地位。为了在竞争中保持不败之地,许多公司往往需要投入大量的人力物力进行前沿技术的前期研究工作,作为公司的技术储备。而研究成果,如电子设计、机械设计等,大量以技术图纸的形式保存,它们的安全保密问题对公司至关重要,但又是一个非常棘手的问题,如何保证既能方便使用、又能保证这些资料的安全,已经成为各大公司亟待解决的问题,为此需要对图像资料进行加密;其次,在Internet已经作为人们或单位之间进行信息交流的主要渠道的今天,为保证图像的安全传送,也需要进行图像的加密和解密。

目前,图像的加密方法大量基于混沌理论,如Logistic系统、Henon系统、Lorenz系统、Hua系统、Chen系统等等,其中一维系统已经被证明安全性不高和密钥空间较小,无法有效抵御穷举攻击。为提高图像的安全性,有研究者把多个混沌系统进行有机结合[1],并采用类似于DES算法对图像进行置乱,这些算法已经取得很好效果。但目前几乎所有的算法都基于像素置乱和加密,尤其是基于像素的置乱加密算法,其安全性有待提高[2]。文中主要研究图像资料的加密问题。和现有的算法不同,本研究首先利用广义Arnold映射对在不同的位平面上原始图像进行保面积映射,其映射矩阵中的元素由Logistic系统组合的二维系统产生的混沌序列作为基本参数形成。然后,采用三维Chen系统产生的混沌序列分别对置乱后的图像的红、绿、兰三基色进行加密。经实验表明,加密/解密效果良好,算法简单,可以抵御各种攻击,同时能够用硬件实现,效率高。

1 基于位平面图像映射置乱

对于一幅大小为$N \times N$的彩色图像g,通常采用可逆、保面积映射进行置乱。映射过程为$\mathrm{map}(x,y)$:$(i,j) \to (k,l)$,即在参数x和y的作用下,把原处于(i,j)像素移动到位置(k,l),以达到对图像置乱的目

收稿日期:2007-02-11
基金项目:福建省教育厅科研基金(JA00423)
作者简介:洪联系(1958-),男,福建南安人,副教授,主要从事智能计算、供应链建模、数字图像加密解密、网络安全等方面研究。

的。为保证被置乱的图像正确还原,要求映射过程是保面积的,且映射 map(x,y) 必须存在相应的逆过程 map$'(x,y):(k,l)\rightarrow(i,j)$。广义 Arnold 映射

$$\begin{bmatrix}k\\l\end{bmatrix}=\begin{bmatrix}k_{11}&k_{12}\\k_{21}&k_{22}\end{bmatrix}\begin{bmatrix}i\\j\end{bmatrix}\bmod N$$
$$i,j,k,l=1,2,\cdots,N \tag{1}$$

可以满足上述要求。为叙述方便,称 $\boldsymbol{M}=\begin{bmatrix}k_{11}&k_{12}\\k_{21}&k_{22}\end{bmatrix}$ 为映射矩阵。在 Arnold 映射中要求 $k_{11}k_{22}-k_{12}k_{21}=1$。为简化映射矩阵构建,通常假设 $k_{11}=1$、$k_{12}=a$ 和 $k_{21}=b$,则 $k_{22}=ab+1$。直到现在,所有采用 Arnold 映射的置乱算法都是在图像级进行置乱[3,4],即置乱的前后像素值没有被改变,此时在已知图像的情况下很容易受到攻击[2],其安全性不佳。为此,本算法采取基于位平面置乱。

首先把一幅原始图像 g 视作由若干个位平面组成,在位平面上用 Arnold 映射对图像进行置乱操作。为了到达像素级置乱效果,在不同的位平面上采用不同的映射矩阵,其映射过程:

$$\begin{bmatrix}k_p\\l_p\end{bmatrix}=\begin{bmatrix}1&a_p\\b_p&a_pb_p+1\end{bmatrix}\begin{bmatrix}i\\j\end{bmatrix}\bmod N$$
$$p=1,2,\cdots,P$$
$$i,j,k_p,l_p=1,2,\cdots,N \tag{2}$$

其中 P 为图像的位平面数,$\{1,a_p,b_p,a_pb_p+1\}$ 为第 p 个位平面上采用的映射矩阵的元素值,由参数 (a_p,b_p) 决定。

为简单起见,算法中利用一维 Logistic 系统定义一个二维非线性动力系统:

$$\begin{cases}x_i=\mu_1x_{i-1}(1-x_{i-1})+\gamma_1y_{i-1}^2\\y_i=\mu_2y_{i-1}(1-y_{i-1})+\gamma_2(x_{i-1}^2+x_{i-1}y_{i-1})\end{cases}$$
$$i=1,2,3,\cdots \tag{3}$$

其中为加大系统的复杂性,在二维非线性动力系统中增加了二次偶合项 x_{i-1}^2、y_{i-1}^2 和 $x_{i-1}y_{i-1}$,当 $2.75<\mu_1\leqslant3.40$,$2.7<\mu_2\leqslant3.45$,$0.15<\gamma_1\leqslant0.21$ 及 $0.13<\gamma_2\leqslant0.15$ 时,该系统进入混沌状态,将生成(0,1.0]的混沌序列。

那么:

$$\begin{cases}a_p=x_p\times10^{12}\bmod K+1\\b_p=y_p\times10^{12}\bmod K+1\end{cases}\quad p=1,2,3,\cdots$$

其中 $2\leqslant K\leqslant10^5$,来产生若干组 $2\sim10^5$ 的整数随机参数$\{a_p,b_p\}$序列,从而形成式(2)中映射矩阵。该序列对初始值(x_0,y_0)十分敏感,不同的(x_0,y_0)将产生完全不同的随机参数序列(a_p,b_p),从而达到像素置乱之目的。

2　图像加密

2.1　加密混沌系统

目前对图形图像加密算法通常采用超混沌加密算法[5],其中常见采用 Lorenz 系统、Chua 系统、Henon 系统和 Chen 系统,其中 Chen 系统具备比 Lorenz 系统、Henon 系统和 Chua 系统更优越的动力特性,且容易用电路实现[6~9],因此,本算法采用 Chen 系统:

$$\begin{cases}\dfrac{dx}{dt}=a(y-x)\\\dfrac{dx}{dt}=-xz+by+x(b-a)\\\dfrac{dx}{dt}=xy-cz\end{cases} \tag{4}$$

其中 $a=35,b=28,c=3$。从系统的相轨迹图可以看出,该系统在相空间具有非常优越的三维动力特性。

2.2　离散混沌序列

离散混沌序列产生采用如下步骤:

(1)应用四阶 Runge－Kutta 法,取初始值为 (x_0,y_0,z_0) 和分步步长为 0.01 对 Chen 系统进行数值积分,每个步长得到一组实数数值,该组数据是随机性较好的实数型数值系列(x_i,y_i,z_i),$i=1,2,\cdots,M$,作为初始的混沌信号系列。

(2) 对该混沌信号进行放大、量化和模运算:

$$\begin{cases}nx_i=x_i\times10^{18}\bmod256\\ny_i=y_i\times10^{18}\bmod256\\nz_i=z_i\times10^{18}\bmod256\end{cases}\quad i=1,2,\cdots,M \tag{5}$$

得到一组取值范围为 0～255 的(nx_i,ny_i,nz_i),$i=1,2,\cdots,M$ 整数混沌序列,因为该序列是经过放大后模运算得到的,对初始值(x_0,y_0,z_0)非常敏感;其次,该序列是经过放大和模运算得到,无法从(nx_i,ny_i,nz_i)推出$(nx_{i+1},ny_{i+1},nz_{i+1})$或$(nx_{i-1},ny_{i-1},nz_{i-1})$,因为从$(nx_i,ny_i,nz_i)$推出$(x_i,y_i,z_i)$的唯一途径是穷举,但其空间非常大,无法实现。

2.3　加密操作

为保证序列更具随机性,在整数混沌序列(nx_i,ny_i,nz_i)中去掉迭代过程的前4000个点,取(nx_i,ny_i,nz_i),$i=4000,4001,\cdots,M$ 的整数混沌系列,组成 $N\times N$ 的矩阵形式$(kx_{ij},ky_{ij},kz_{ij})$,用该系列与置乱后图像 g' 中各个像素的红、绿、兰三基色进行异或操作:

$$\begin{cases}\text{Cred}'_{ij}=\text{Cred}_{ij}\oplus kx_{ij}\\\text{Cgreen}'_{ij}=\text{Cgreen}_{ij}\oplus ky_{ij}\\\text{Cblue}'_{ij}=\text{Cblue}_{ij}\oplus kz_{ij}\end{cases}\quad\begin{matrix}i=1,2,\cdots,N\\j=1,2,\cdots,N\end{matrix} \tag{6}$$

其中 $\oplus$ 为异或运算符。经过加密得到加密后的彩色图像 $g''(\text{Cred}'_{ij},\text{Cgreen}'_{ij},\text{Cblue}'_{ij})$,$i,j=1,2,\cdots,N$。由于 Chen 系统对初始点$(x_0,y_0,z_0)$十分敏感,初始点有

微小变化将产生不同序列。用不同的初始点(x_0^p, y_0^p, z_0^p)，$p = 1,2,\cdots,m$，经过上述处理将产生不同的离散混沌系列$(kx_{ij}^p, ky_{ij}^p, kz_{ij}^p)$，$p = 1,2,\cdots,m$，用这些混沌系列对原始图像进行多次异或运算加密：

$$\begin{cases} \text{Cred}'_{ij} = \text{Cred}_{ij} \oplus kx_{ij}^1 \oplus kx_{ij}^2 \oplus \cdots \oplus kx_{ij}^m \\ \text{Cgreen}'_{ij} = \text{Cgreen}_{ij} \oplus ky_{ij}^1 \oplus ky_{ij}^2 \oplus \cdots \oplus ky_{ij}^m \\ \text{Cblue}'_{ij} = \text{Cblue}_{ij} \oplus kz_{ij}^1 \oplus kz_{ij}^2 \oplus \cdots \oplus kz_{ij}^m \\ i = 1,2,\cdots,N \\ j = 1,2,\cdots,N \end{cases} \tag{7}$$

得到对此加密后的图像 g''。

图像加密/解密过程如图1所示。整个加密过程和解密过程除 Arnold 置乱映射和逆映射不同外，其他部分完全一致。一般情况下，Arnold 逆映射要计算该映射周期后才能确定逆映射次数，而且该映射周期与被处理图像大小不是成正比关系，为提高 Arnold 逆映射的速度和效率，文献[10]采用一种 Arnold 逆映射的新算法，但该算法不适用广义 Arnold 的逆映射且效率不高。观察式(1)不难发现，Arnold 映射过程是把原图像位置(i,j)上的像素映射到(k,l)位置上，那么其逆映射即为把(k,l)的像素映射到(i,j)位置上。因此，完全可以用原来式(1)的映射过程，通过(i,j)求得(k,l)后，把位置(k,l)上的像素移动到(i,j)上便实现逆映射过程。该逆映射方法简单，不需要进行判断，不仅可以适用于经典的 Arnold 映射，也适用于广义 Arnold 映射，无论是二维或三维均可以实现，而且计算时间比文献[10]大大缩短。因此，本算法采用的加密/解密过程基本一致。

进行 Arnold 映射和逆映射过程中，由于每次的映射过程采用的密钥(x_0, y_0)产生不同参数(a_p, b_p)序列，而产生不同的置乱效果，因此要求逆映射过程输入(x_0, y_0)的顺序与原映射过程的输入(x_0, y_0)顺序相反，否则将无法还原。

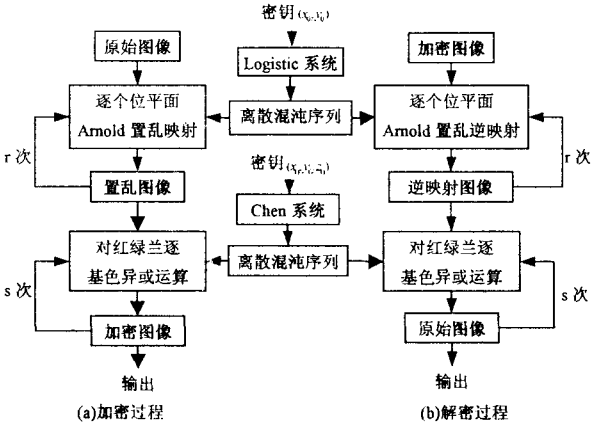
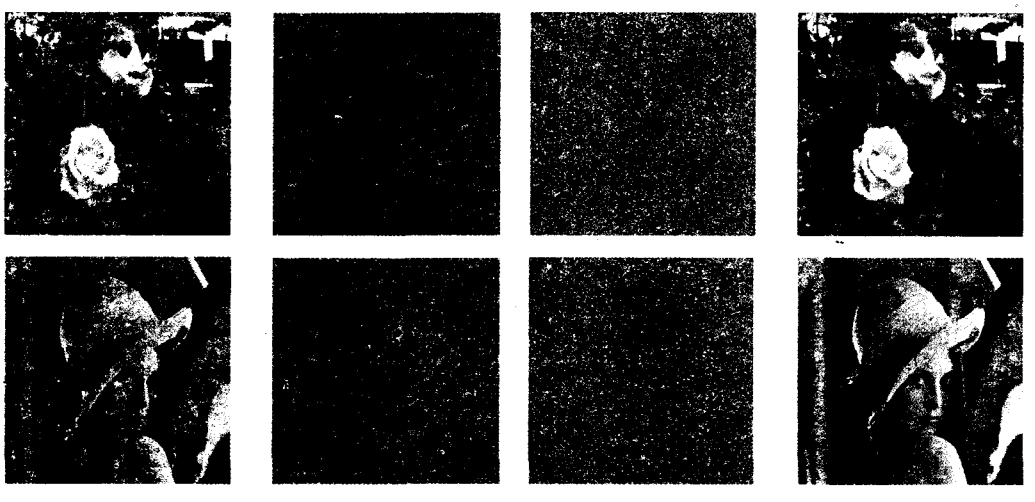


图 1 彩色图像加密/解密过程

3 计算实例与安全性分析

为了检验本算法的计算效果，把上述过程用 Visual C# 实现、在 Pentiuum4 1.3GHz CPU、Windows XP 操作下运行，分别对玫瑰花和 Lena 图像进行加密和解密操作，操作结果如图 2 所示。经过位平面置乱后的图像各个像素值已经被完全破坏，加密后的图像从直观视觉效果上看几乎一样，而且可以实现完全不失真解密还原。同时，该算法具有如下特点：

(1)密钥空间巨大。基于 Chen 混沌系统和 Logistic 系统对初始值(x_0, y_0, z_0)和(x_0, y_0)非常敏感，只要取值得当，初始值一个非常小的变化都可以产生完全不同的混沌系列。在 Visual C# 上，计算原始混沌系列中 Chen 系统的(x_i, y_i, z_i)和 Logistic 系统的(x_i, y_i)均采用 Decimal 数值类型，当初始值误差为10^{-18}时，便产生不同的混沌系列。同时每组密钥有五个值(即 Log-



(a) 原始图像 (b)置乱后图像 (c)多次加密图像 (d) 解密图像

图 2 加密/解密效果

istic 系统中的(x_0, y_0)和 Chen 系统中的(x_0, y_0, z_0)),它们在实数域中的取值不受任何限制,同时允许多次加密,具有非常大的密钥空间。

(2)具有良好的抵御统计攻击能力。对图像加密的另一种方法就是对图像进行直方图分析。图 3 为 Lena 图像加密前后的统计直方图。图像加密后其各个颜色值均匀分布,平均基色值在(127.42～127.53)之间,原始图像的统计分布被破坏。

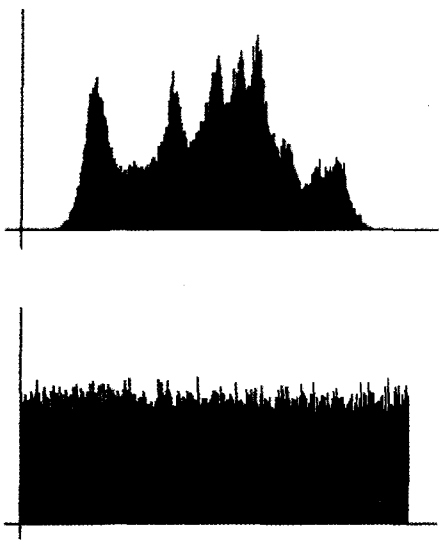


图 3　统计直方图分析

(3)能够有效抵御相关分析攻击。随机取一些点,以每个点为中心,计算其相邻各个点颜色值数学期望值、自相关和互相关,以及协方差[11]。

每种颜色的自相关分析:

$$E_x(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=j-3}^{j+3} x_{pq}$$

$$R_x(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=j-3}^{j+3} (x_{pq} - E(x_{ij}))^2$$

颜色之间的互相关分析:

$$R_{xy}(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=i-3}^{i+3} (x_{pq} - E(x_{ij}))(y_{pq} - E(y_{ij}))$$

$$\eta_{xy}(i,j) = \frac{R_{xy}(i,j)}{\sqrt{R_x(i,j)R_y(i,j)}}$$

上述计算分别取像素(i,j)为中心的 7×7 点阵进行分析,分析结果如图 4 所示为彩色图像加密前后的邻域相关分析,从随机选取的 6000 个像素分析可以看出,原彩色图像的大部分像素的邻域相关性在 1.0 附近,而加密后的彩色图像各个像素的颜色值相关性仍然很小。因此,该加密方法可以非常有效抵御采用相关分析的攻击。

4　结　论

提出一种把 Arnold 映射、Logistic 系统和 Chen 系统有机结合的多混沌系统图像加密算法,和其他算法不同,本算法采用在位平面进行多次 Arnold 映射和对不同基色进行多次加密,算法可以实现对彩色图像进行加密和解密;该算法简单、易用硬件实现,加密/解密效率高;该加密算法的安全性仅取决于密钥,且有足够大的密钥空间,完全可以抵御穷举等各种攻击,已经在某公司技术图纸的加密/解密上得到应用。

参考文献:

[1] 朱从军,李　力,陈志刚.基于多维混沌系统组合的图像加密新方法[J].计算机工程,2007,33(2):142－144.

[2] 郭建胜,金晨辉.对基于广义猫映射的一个图像加密系统的已知图像攻击[J].通信学报,2005,26(2):131－135.

[3] 马在光,丘水生.基于广义猫映射的一种图像加密系统[J].通信学报,2003,24(2):51－57.

[4] 刘　英,孙丽莎.基于三维猫映射图像加密算法[J].计算机工程与应用,2005(36):127－130.

[5] 李雄军,彭建华.基于二维超混沌图像加密算法[J].中国图像图形学报,2003,8(10):1172－1177.

[6] 张丽丽,雷友发.一个三维非线性系统的混沌动力学特征[J].动力学与控制学报,2006,4(1):5－7.

[7] Chen G, Dong X. From Chaos to Order Methodologies: Perspectives and Application[M]. Singapore: World Scientific Pub. Co, 1998.

[8] Ueta T, Chen G R. Bifurcation Analysis of Chen's Equation [J]. International Journal Bifurcation and Chaos, 2000, 10 (8):1917－1931.

[9] Yassen M T. Chaos Control of Chen Chaotic Dynamical System[J]. Chaos, Solitons & Fractals, 2003, 15(2):271－283.

[10] 孔　涛,张　亶.Arnold 反映射的一种新算法[J].软件学报,2004,15(10):1558－1564.

[11] Chen Guanrong, Mao Yaobin, Charles K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons and Fractals, 2004, 21(3):749－761.

(上接第 69 页)

Workshops 2003. Providence, Rhode Island, USA: [s. n.], 2003.

[5] Intanagonwiwat C, Govindan R, Estrin D, et al. Directed Diffusion for Wireless Sensor Networking[C]// ACM/IEEE (MOBICOM 2000). New York, NY, USA: ACM Press, 2000.

[6] 张　悦.无线传感器网络 LEACH 协议群首算法的改进[J].微计算机信息,2006(10):183－185.