文章编号:1001 - 9081(2007)08 - 1891 - 04

扩散映射置乱与超混沌系统组合图像加密算法

洪联系[1],李传目[1],卢明玺[2]
(1. 集美大学 计算机工程学院,福建 厦门 361021; 2. 集美大学 诚毅学院,福建 厦门 361021)
(lxhong@jmu.edu.cn)

摘 要:提出一个基于扩散与位平面 Arnold 映射相结合的彩色图像置乱,以及采用 Chen 系统产生的混沌序列加密的图像加密算法。先由 Logistic 系统构造的二维非线性动力系统产生的混沌序列形成扩散矩阵和 Arnold 映射矩阵,然后在基色上对彩色图像进行扩散,并在不同的位平面对彩色图像进行置乱,最后用 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,能够抵御多种攻击,且容易用硬件实现。

关键词:彩色图像加密;Arnold 映射;灰度值扩散;位平面置乱;Chen 系统
中图分类号: TP309.7 **文献标志码**:A

Combined image encryption algorithm based on diffusion mapped disorder and hyperchaotic systems

HONG Lian-xi[1], LI Chuan-mu[1], LU Ming-xi[2]
(1. *Computer Engineering College, Jimei University, Xiamen Fujian* 361021, *China*;
2. *Chengyi College, Jimei University, Xiamen Fujian* 361021, *China*)

Abstract: A combined image encryption algorithm was presented. The algorithm combined linear diffusion approach with Arnold mapped to disorder the image, and hyperchaotic sequences was used to encrypt the image. The mapped matrix and diffusion matrix were made up of chaotic sequences that were produced by the Logistic dynamic system, and they were used for disordering the color image to produce a disordered image on different bit planes to disorder the pixels. The disordered image was encrypted by means of the hyperchaotic sequences that were produced by the Chen's system. The algorithm is simple and able to resist a variety of attacks, and can be easily implemented by hardware.

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

0 引言

在 Internet 已经作为进行信息交流主要渠道的今天,人们需要在网络上交流大量的信息,其中包括图像资料,为保证图像的安全传送,在传送过程中要进行图像的加密和解密处理。目前,图像的加密方法大量基于混沌理论,如一维 Logistic 系统、Henon 系统、Lorenz 系统、Hua 系统和 Chen 系统等,其中一维系统已经被证明安全性不高且密钥空间较小,不能有效抵御穷举攻击。为提高图像加密的安全性,有研究者把多个混沌系统进行有机结合[1],或采用多维 Arnold 映射对图像进行置乱,这些算法已经取得了很好的效果。但目前几乎所有的置乱算法都是基于图像级置乱[2-4],此时图像的统计特性没有变化,其安全性有待提高[4];其次有些加密算法[1,5]采用混沌序列直接与像素的灰度值直接叠加,原图像像素的位置没有变化,容易受到像素的相关分析攻击,尤其是图像像素灰度级比较少的设计图。

从信息论的观点出发,本文提出灰度值扩散与位平面映射相结合的方法对图像进行置乱,接着用超混沌序列对置乱的图像进行加密。算法首先利用扩散算法和广义 Arnold 映射,对不同基色进行扩散和在不同的位平面上对原始图像进行映射,实现在像素级上进行图像置乱。然后采用三维 Chen 系统产生的混沌序列分别对置乱后图像的红、绿、蓝三基色进行加密。实验结果表明,加密/解密效果良好,算法简单,可以抵御各种攻击。

1 图像置乱

在图像加密系统中,采用非线性函数映射置乱和线性变换进行扩散,可以有效抵御对加密系统进行的统计分析攻击。为此,扩散算法和映射算法被引进对图像进行置乱。

1.1 扩散置乱

所谓扩散置乱,是指把图像中像素的灰度值用某种算法扩散到相邻的若干个像素上的图像置乱操作。对于一幅大小为 $N \times N$ 的彩色图像 G,采用两邻点相互扩散的线性变换算法:

$$\begin{bmatrix} g_{ij}' \\ g_{i,j+1}' \end{bmatrix} = [\boldsymbol{D}] \begin{bmatrix} g_{ij} \\ g_{i,j+1} \end{bmatrix} \bmod K \tag{1}$$

对图像像素的灰度值进行扩散。其中 $\boldsymbol{D} = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix}$ 称为 2 × 2 扩散矩阵,g_{ij} 和 $g_{i,j+1}$ 分别为原图像点 (i,j) 和 $(i,j+1)$ 处的三基色值,g_{ij}' 和 $g_{i,j+1}'$ 分别为扩散后的三基色值,K 为图像的基色级,mod 为模运算(下同)。为简化逆扩散运算,通常取 $|\boldsymbol{D}| = 1$,且令 $d_{11} = 1$、$d_{12} = a_s$、$d_{21} = b_s$,则 $d_{22} = a_s b_s + 1$,称

收稿日期:2007 - 02 - 15;**修回日期**:2007 - 04 - 29。 **基金项目**:福建省教育厅科研基金资助项目(JA00423)。

作者简介:洪联系(1958 -),男,福建南安人,副教授,博士研究生,主要研究方向:智能计算、供应链建模、数字图像加密解密、网络安全;李传目(1966 -),男,河南范县人,副教授,硕士,主要研究方向:计算机网络安全和信息加密; 卢明玺(1984 -),女,江西赣州人,硕士研究生,助理实验师,主要研究方向:通信系统安全。

它们为扩散加权系数,取整数,由参数序列$\{(a_s,b_s)\}(s=1,2,\cdots,r)$决定,其中$r$为扩散置乱次数。那么其逆扩散为:

$$\begin{bmatrix} g_{ij} \\ g_{i,j+1} \end{bmatrix} = [\boldsymbol{D}]^{-1}\begin{bmatrix} g_{ij}' + m \times K \\ g_{i,j+1}' + n \times K \end{bmatrix} \tag{2}$$

其中m和n为能使得$0 \leqslant g_{ij} < K$和$0 \leqslant g_{i,j+1} < K$的最小整数值。如果采用三邻点扩散,则$\boldsymbol{D}$为$3\times3$扩散矩阵,大于三邻点扩散时$\boldsymbol{D}$构造比较复杂,一般不用。

应用式(1)多次对图像自(0,0)开始逐行扩散,得到扩散后的图像。通常取$d_{12} \geqslant 2$,这样图像中每个像素的灰度值将被放大扩散到整幅图像中,算法对被加密图像敏感。

逆扩散则应用式(2)从$(N-1,N-1)$开始对扩散后的图像逐行反方向扩散,进行图像还原。

1.2 映射置乱

所谓映射置乱是把原始图像中的像素从一个位置映射到另一个位置的置乱操作。在图像加密置乱中的映射置乱要求可逆,如映射过程为$\mathrm{map}(x,y):(i,j)\rightarrow(k,l)$,即在参数$x$和$y$的作用下,把原处于$(i,j)$的像素移动到位置$(k,l)$,以达到对图像置乱的目的;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$\mathrm{map}(x,y)$必须存在相应的逆过程$map'(x,y):(k,l)\rightarrow(i,j)$。广义 Arnold 映射:

$$\begin{bmatrix} k \\ l \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}\begin{bmatrix} i \\ j \end{bmatrix} \bmod N;\ i,j,k,l = 1,2,\cdots,N \tag{3}$$

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。在广义 Arnold 映射中,要求$|\boldsymbol{M}| = 1$。为简化映射矩阵构建,通常假设$k_{11}=1$、$k_{12}=d$和$k_{21}=e$,则$k_{22}=de+1$。

到目前为止,所有采用 Arnold 映射的置乱算法都是在图像级进行置乱[2,3]。所谓图像级置乱,就是直接把图像的像素从一点映射到另一点以达到图像被置乱的目的,其置乱前后像素灰度值的统计特征没有被改变,这样在已知图像的情况下很容易受到攻击[4],其安全性不佳,为此,本算法采取基于位平面置乱。所谓基于位平面置乱,是把一幅原始图像G视作由若干个位平面组成(如256级的灰色图像有8个位平面),在每个位平面上用 Arnold 映射对图像中各像素的比特位进行置乱操作。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:

$$\begin{bmatrix} k_p \\ l_p \end{bmatrix} = \begin{bmatrix} 1 & d_p \\ e_p & d_pe_p+1 \end{bmatrix}\begin{bmatrix} i \\ j \end{bmatrix} \bmod N;\ p = 1,2,\cdots,P,\ i,j,\ k_p,l_p = 1,2,\cdots,N \tag{4}$$

其中P为图像的位平面数,$\{1,d_p,e_p,d_pe_p+1\}$为第p个位平面上所采用的映射矩阵的元素值,由参数序列$\{(d_p,e_p)\}$决定。由于采用不同映射矩阵,同一像素中的各个比特位将被映射到不同的位置上,从而达到像素级置乱的目的,也就是说,映射过程除了像素被置乱,同时各像素的灰度值也被置乱,原始图像的统计特征完全被破坏。

一般情况下,Arnold 逆映射要计算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的大小并不成正比关系,为提高 Arnold 逆映射的速度和效率,文献[6]提出一种 Arnold 逆映射的新算法,但该算法不适用于广义 Arnold 的逆映射,且效率不高。观察式(3)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,可以用式(3)的映射过程由(i,j)求得(k,l)后,把位置(k,l)上的像素移动到(i,j)上即实现广义 Arnold 的逆映射过程。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适用,而且计算时间比文献[6]大大缩短。

1.3 参数生成

在扩散置乱和映射置乱操作中,其置乱效果分别由参数序列$\{(a_s,b_s)\}$和$\{(d_p,e_p)\}$决定,为简化用户操作,同时也使得扩散和映射操作完全依赖于若干个密钥,算法中利用一维 Logistic 系统定义一个二维非线性动力系统:

$$\begin{cases} x_i = \mu_1 x_{i-1}(1-x_{i-1}) + \gamma_1 y_{i-1}^2 \\ y_i = \mu_2 y_{i-1}(1-y_{i-1}) + \gamma_2(x_{i-1}^2 + x_{i-1}y_{i-1}) \end{cases};\ i = 1,2,\cdots \tag{5}$$

来生成这些参数序列。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$2.75 < \mu_1 \leqslant 3.40$,$2.7 < \mu_2 \leqslant 3.45$,$0.15 < \gamma_1 \leqslant 0.21$以及$0.13 < \gamma_2 \leqslant 0.15$时,该系统进入混沌状态,生成(0,1.0]的混沌序列。那么:

$$\begin{cases} Cx_p = x_p \times 10^{12} \bmod K + 1 \\ Cy_p = y_p \times 10^{12} \bmod K + 1 \end{cases};\ p = 1,2,3,\cdots$$

其中K的大小取决于扩散操作或映射操作。一般在扩散操作时取较小值,而在映射操作时取较大值。把生成的若干组整数类随机参数$\{(Cx_p,Cy_p)\}$作为$\{(a_s,b_s)\}$和$\{(d_p,e_p)\}$参数序列。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$\{(a_s,b_s)\}$和$\{(d_p,e_p)\}$,从而到达图像置乱之目的。

2 图像加密

2.1 加密混沌系统

图形图像加密算法比较多采用超混沌加密算法[5],常见的有 Lorenz 系统、Chua 系统、Henon 系统和 Chen 系统,其中 Chen 系统具备比其他三者更优越的动力特性,且容易用电路实现[7-9],因此,本算法采用 Chen 系统:

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = a(y-x) \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = -xz + by + x(b-a) \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = xy - cz \end{cases} \tag{6}$$

其中当$a=35$,$b=28$,$c=3$时,系统进入混沌状态,其相空间具有非常优越的三维动力特性[10]。

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,该组数据类随机的实数型数值序列$(x_i,y_i,z_i)(i=1,2,\cdots,M)$,作为初始的混沌信号序列。

2)对该混沌信号进行放大、量化和模运算:

$$\begin{cases} nx_i = x_i \times 10^{18} \bmod K \\ ny_i = y_i \times 10^{18} \bmod K \\ nz_i = z_i \times 10^{18} \bmod K \end{cases};\ i = 1,2,\cdots,M \tag{7}$$

得到一组取值范围为$0 \sim (K-1)$的$(nx_i,ny_i,nz_i)(i=1,2,\cdots,M)$整数混沌序列,$K$为图像各基色的灰度级。因为该序列是经过放大后模运算得到的,因此它对初始值(x_0,y_0,z_0)非常敏感;而且由于空间非常大,使得攻击者无法从(nx_i,ny_i,nz_i)推出$(nx_{i+1},ny_{i+1},nz_{i+1})$或$(nx_{i-1},ny_{i-1},nz_{i-1})$。

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$(nx_i,ny_i,nz_i)(i=4001,$

4002,…,M) 的整数混沌序列,组成 $N \times N$ 的矩阵形式(kx_{ij}, ky_{ij},kz_{ij}),然后用该序列与置乱后图像 G' 中各个像素的红、绿、兰三基色进行异或操作:

$$\begin{cases} Cred_{ij}' = Cred_{ij} \oplus kx_{ij} \\ Cgreen_{ij}' = Cgreen_{ij} \oplus ky_{ij} \\ Cblue_{ij}' = Cblue_{ij} \oplus kz_{ij} \end{cases} ; i = 1,2,\cdots,N, j = 1,2,\cdots,N \tag{8}$$

得到加密后的彩色图像 $G'(Cred_{ij}', Cgreen_{ij}', Cblue_{ij}')(i, j = 1,2,\cdots,N)$,其中 $\oplus$ 为异或运算符。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完全不同的离散混沌序列 $(kx_{ij}^p, ky_{ij}^p, kz_{ij}^p)(p = 1,2,\cdots,m)$,用这些混沌序列对原始图像进行多次异或运算:

$$\begin{cases} Cred_{ij}' = Cred_{ij} \oplus kx_{ij}^1 \oplus kx_{ij}^2 \oplus \cdots \oplus kx_{ij}^m \\ Cgreen_{ij}' = Cgreen_{ij} \oplus ky_{ij}^1 \oplus ky_{ij}^2 \oplus \cdots \oplus ky_{ij}^m \\ Cblue_{ij}' = Cblue_{ij} \oplus kz_{ij}^1 \oplus kz_{ij}^2 \oplus \cdots \oplus kz_{ij}^m \end{cases} ; i = 1,2,\cdots,N, j = 1,2,\cdots,N \tag{9}$$

得到最终的加密后图像 G'。

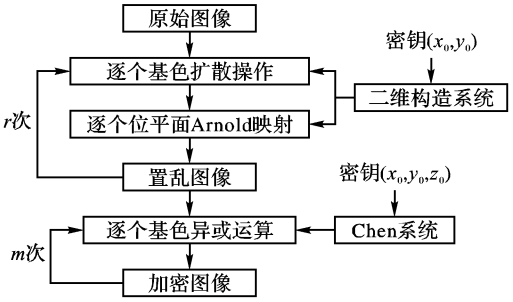


图 1　图像加密过程

图像置乱加密过程如图 1 所示。整个加密过程包括置乱和加密两部分。首先在密钥 (x_0, y_0) 作用下通过二维构造系统(如式(5)所示)产生的离散混沌序列,应用式(1)对原图像的基色值进行扩散,应用式(3)在位平面上进行广义 Arnold 映射,扩散与映射交替进行 r 次,r 值取决于图像要求的安全级别,一般 $r = 3$ 已经足够。然后在另一组密钥 (x_0, y_0, z_0) 作用下通过 Chen 系统(如式(6)所示)和式(7)生成的混沌序列应用式(9)对置乱后的图像进行多次异或运算,以实现对图像的加密。

3　图像的解密

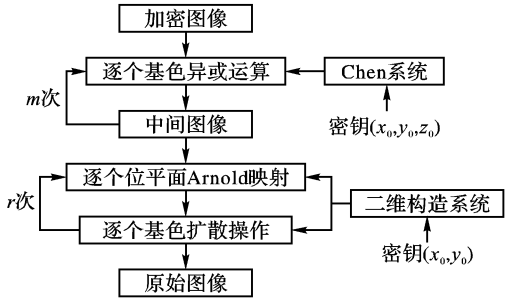


图 2　图像解密过程

整个解密过程如图 2 所示。首先在密钥的作用下通过 Chen 系统和式(7)产生混沌序列,应用式(9)对加密后的图像进行解密。由于对图像的加密/解密采用的是异或运算,加密和解密过程完全一致,且在解密过程中只要密钥输入正确,与密钥的输入顺序无关。

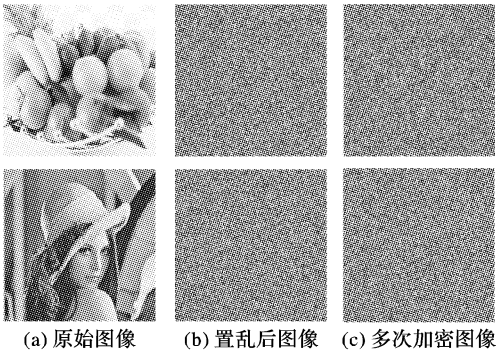
接着在位平面上进行广义 Arnold 的逆映射。如 1.2 节所述,由于直接求 Arnold 的逆映射比较困难,在本算法中,直接应用式(4)通过 (i, j) 求得 (k, l),然后把位于像素 (k, l) 上对应的比特位映射到 (i, j) 像素上对应的比特位来实现广义 Arnold 的逆映射。在进行 Arnold 逆映射过程中所使用的密钥序列要求和置乱时使用的序列顺序相反。

最后应用式(2)对图像的各个基色进行逆扩散操作。为了提高加密算法的安全性能,在加密过程中采用扩散和 Arnold 映射操作交替进行,解密过程则要求 Arnold 逆映射和扩散交替进行。

4　计算实例与安全性分析

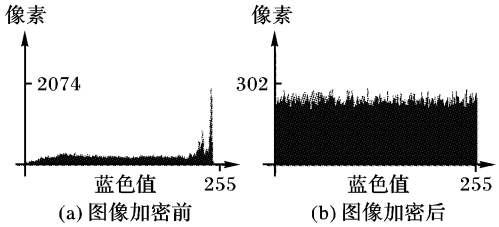
为了检验本算法的计算效果,在 Pentium 4 1.3 GHz CPU,内存为 384 MB, Windows XP 操作系统下,用 Visual C#实现上述过程,分别对彩色水果篮和灰色的 Lena 图像(均为 256 × 256 幅度)进行加密和解密操作,结果如图 3 所示。经过扩散和位平面置乱后的图像各个像素值已经被完全破坏,加密后的图像从直观视觉效果上看几乎一样,且可以实现完全不失真解密还原,还原结果与原始图像完全一致。同时,该算法具有如下特点:

1)密钥空间巨大。因为 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序列。在 Visual C#上,计算原始混沌序列中 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,便产生不同的混沌序列。也就是说,解密密钥和加密密钥只要有 10^{-18} 的差别就无法进行解密。同时每组密钥有五个值(即二维构造系统中的 (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,可以抵御密钥穷举攻击。



(a) 原始图像　(b) 置乱后图像　(c) 多次加密图像

图 3　加密效果



(a) 图像加密前　(b) 图像加密后

图 4　彩色水果篮统计直方图分析

2)具有良好地抵御统计攻击能力。对图像加密的另一种攻击方法就是对图像进行直方图分析。图 4 所示为水果篮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),像素较均匀分布在各个基色值上,最大像素个数为 302 个。由此可见,加密后的图像的统计分布完全被破坏,具有很好地抵御统计分析的能力。

3)能够有效抵御像素相关统计分析攻击。为了说明加密后图像的相关特征被完全破坏,采用文献[11]提供的相关分析方法。随机取一些点,以该点为中心,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。每种颜色的自相关值为:

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

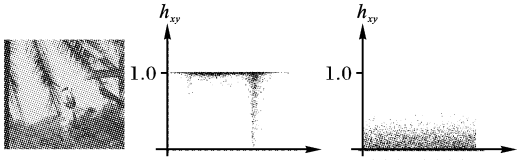
$$R_x(i,j) = \frac{1}{49}\sum_{p=i-3}^{i+3}\sum_{q=j-3}^{j+3} (x_{pq} - E(x_{ij}))^2$$

颜色之间的互相关值为:

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

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

应用上述计算公式,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5所示。图中给出彩色图像加密前后随机选取的6000个像素邻域相关分析结果。可以看出,原图像的大部分像素的邻域相关性在1.0附近,而加密后的图像各个像素的颜色值相关性非常小,因此,该加密方法可以有效地抵御采用像素相关分析的攻击。



(a) 原始图像 (b) 原图相关分析 (c) 加密后相关分析

图5 彩色图像邻域相关分析

5 结语

提出一个把扩散、Arnold映射、Logistic系统和Chen系统有机结合的多混沌系统图像置乱加密算法。从信息论出发,算法首先对图像进行扩散和在位平面进行多次Arnold映射,实现对图像的置乱操作,然后用Chen系统产生的超混沌序列对不同基色进行多次加密,可以实现对各种图像进行加密和解密。该算法简单、易用硬件实现;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,在完全公开算法的情况下,能够有效抵御各种攻击。相应的算法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.

[2] 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.

[3] 刘英,孙丽莎.基于三维猫映射的图像加密算法[J].计算机工程与应用,2005,41(36):127-130.

[4] 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.

[5] 李雄军,彭建华,徐宁,等.基于二维超混沌的图像加密算法[J].中国图象图形学报:A版,2003,8(10):1172-1177.

[6] 孔涛,张亶.Arnold反映射的一种新算法[J].软件学报,2004,15(10):1558-1564.

[7] CHEN G, DONG X. From chaos to order methodologies: perspectives and application[J]. Singapore: World Scientific, 1998, 24(16):760-767

[8] UETA T, CJHEN G R. Bifurcation analysis of Chen's equation[J]. International Journal Bifurcation and Chaos, 200, 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] 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.

[11] CHEN G R, MAO Y B, CHARLES K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 3(21): 749-761.

[12] 徐江峰,杨有,黄小粟.基于广义同步混沌的图像加密方案[J].计算机工程,2006,32(6):154-156.

[13] CHEN G, UETA T. Yet another chaotic attractor[J]. International Journal of Bifurcation and Chaos, 1999, 9(7):1465-1466.

(上接第1890页)

4 结语

利用统一混沌系统模型结合广义猫映射,提出了基于高维非线性混沌系统实现彩色图像像素置乱和替代加密的新算法。算法具有以下主要优点:

1)实现了对彩色图像三基色分量分别置乱,置乱算法不仅能打破相邻像素的相关性,而且能混淆彩色图像每一像素的R、G、B三元素,使加密图像在视觉上发生了色彩变化,图像保密性更高。

2)像素的位置置换和像素值的替代均基于复杂非线性高维混沌系统,克服了一维混沌系统不能抵御相空间重构攻击的缺点;且以三维统一混沌系统的系统参数和初值为密钥,大大拓展了密钥空间,使算法具有抵御穷举攻击的能力。

3)统一混沌系统具有复杂的非线性混沌行为,因此生成的密钥具有较高的复杂性;且每次随机产生的密钥不同,具有一次一密特性;密文具有在整个取值空间均匀分布的特性,相邻像素具有近似于零的相关性。

混沌加密和解密的速度是较快的,但求解高维混沌系统微分方程的时间开销较大。如果将其用于对网络通信的实时图像加密,可以离线生成混沌序列,然后进行在线加密。这样,算法既具有图像加密的实时性,又确保了加密效果的高安全性。

参考文献:

[1] GUAN Z H, HUANG F J, GUAN W J. Chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1-3): 153-157.

[2] 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.

[3] LONG M, 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.

[4] 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.

[5] WANG S H, KUANG J Y, LI J H, *et al.* Chaos-based communications in a large community[J]. Physical Review E-Statistical, Nonlinear, and Soft Matter Physics, 2002, 66(6): 1-4.

[6] Lü J H, CHEN G R, ZHANG S C. The compound structure of a new chaotic attractor[J]. Chaos, Solitons and Fractals, 2002, 14(5):669-672.

[7] CHEN G R, MAO Y B, CHARLES K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21(3):749-761.