基于高维混沌系统组合的图像加密新算法

李 云,韩凤英
LI Yun,HAN Feng-ying

长沙航空职业技术学院,长沙 410014
Changsha Aeronautical Vocational and Technical College,Changsha 410014,China

LI Yun,HAN Feng-ying.New image encryption algorithm based on combined high-dimension Chaotic system.Computer Engineering and Applications,2009,45(1):103-104.

Abstract: A new image encryption algorithm based on combined high-dimension chaotic system is presented.Firstly,it uses the generalized cat mapping to diffuse the image,then it uses the Lorenz system to confuse the diffused image.The results demonstrate that the algorithm has good properties of confusion and diffusion.The key space is large enough to resist the brute-force attack.For the encrypted image the distribution of pixel-values has a random-like behavior and the values of adjacent pixels satisfy zero correlation,showing that the proposed scheme is of relatively high security.

Key words: Chaotic;image encryption;generalized cat mapping;Lorenz;confusion;diffusion

摘 要:提出了一种基于高维混沌系统组合的图像加密算法。该算法首先利用广义猫映射对图像进行置乱,然后利用 Lorenz 系统对置乱后的图像进行替代变换。研究结果表明,该算法具有良好的像素值混淆、扩散性能和较大抵抗强力攻击的密钥空间,加密图像像素值具有类随机均匀分布特性,且相邻像素的值具有零相关特性。这些结果表明所提出的方案具有较高安全性。

关键词:混沌;图像加密;广义猫映射;Lorenz;替代;置乱
DOI:10.3778/j.issn.1002-8331.2009.01.030 **文章编号**:1002-8331(2009)01-0103-02 **文献标识码**:A **中图分类号**:TP393.08

随着互联网技术与多媒体技术的飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段,信息的安全与保密显得越来越重要。对于多媒体信息,尤其是图像和声音信息,传统的加密技术将其作为普通数据流进行加密,而不考虑多媒体数据的特点,因此有一定的局限性。近年来已有很多学者提出基于混沌系统的图像置乱加密方法[1-4],他很好地克服了传统图像加密方法秘密不能全部寓于密钥之中的缺陷。一维混沌系统具有形式简单,产生的混沌时序时间短等优点,但密钥空间太小,不能有效地抵御穷举攻击[5]。因此有必要探索基于高维混沌系统乃至超维混沌系统的图像加密算法。利用广义猫映射、Lorenz 高维混沌系统结构复杂、多输出、密钥空间大等优点,提出一种基于高维混沌系统组合的图像加密算法,该算法能够有效地抵御穷举攻击、统计分析攻击,算法效率高,具有很好的安全性。

1 广义猫映射的图像置乱算法

将猫映射推广,得到下列广义猫映射公式:

$$\begin{pmatrix}x_n\\y_n\end{pmatrix}=\begin{pmatrix}a & b\\c & d\end{pmatrix}^n\begin{pmatrix}x_0\\y_0\end{pmatrix}\bmod N \tag{1}$$

由式(1)知,该映射存在一个不动点(0,0),即点(0,0)经过 n 次迭代映射后不变,为避免产生不动点,对坐标点的取值改用 $\{1,2,\cdots,N\}\times\{1,2,\cdots,N\}$ 表示,并将映射方程改造为含两个独立参数的形式:

$$\begin{pmatrix}x_n\\y_n\end{pmatrix}=\begin{pmatrix}1 & p\\q & pq+1\end{pmatrix}^n\begin{pmatrix}x_0\\y_0\end{pmatrix}\bmod N+1 \tag{2}$$

可以证明式(2)具有混沌映射的某些特性,而且是一一映射。在图像置乱算法中,利用式(2)来置乱图像像素点的位置:将原始明文图像的像素坐标 (i,j) 作为初值 (x_0,y_0),用给定系数矩阵(由独立参数 p,q 决定)和迭代次数 n 作密钥,生成的迭代结果 (x_n,y_n) 作为原图像点 (i,j) 处像素置换后的新位置 (i',j'),重复上面的步骤直到所有的像素点均被置乱。由于映射的混沌特性,当迭代次数足够大时,任意两个相邻的像素点,它们的新位置将会产生极大的分离;又由于该映射是一一映射,不同位置的明文像素置乱到密文图像空间的位置不会重叠。这样,原始图像的全部像素将被随机而均匀地置乱到密文图像的整个像素空间。

2 Lorenz 系统的图像像素值替代变换

Lorenz 系统是经典的三维混沌系统,以 Lorenz 系统生成加密混沌序列有三大优点:一是系统结构较低维系统复杂,系统变量的实数值序列更不可预测;二是对系统输出的实数值混沌序列进行处理,可产生单变量或多变量组合的加密混沌序列,使得加密序列的设计非常灵活;三是系统的三个初始值和三个

基金项目:湖南省自然科学基金(the Natural Science Foundation of Hunan Province of China under Grant No.06JJ50098);湖南省教育厅资助科研课题(the Research Project of Department of Education of Hunan Province,China under Grant No.07D005)。
作者简介:李云(1973-),女,讲师,从事图形图像研究;韩凤英(1975-),女,讲师,从事混沌密码学研究。
收稿日期:2008-08-05 **修回日期**:2008-11-03

参数都可以作为生成加密混沌序列的种子密钥,若设计过程中再加入部分控制变量,加密算法的密钥空间将大大高于低维混沌系统。Lorenz 系统的动力学方程为:

$$\begin{aligned} dx/dt&=\sigma(y-x)\\ dy/dt&=rx-zx-y\\ dz/dt&=xy-bz \end{aligned} \tag{3}$$

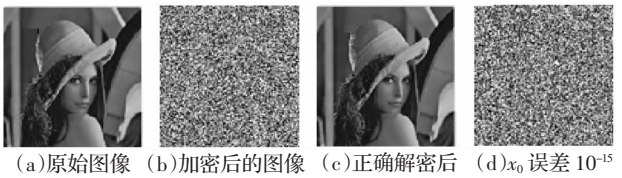
其中,σ,r,b 为系统参数,典型值为 $\sigma=10,r=28,b=8/3$。在保持 σ,b 不变,$r>24.74$ 时 Lorenz 系统进入混沌态[6]。

算法中使用 Lorenz 混沌系统产生的混沌序列对经过置乱变换后的图像进行逐点加密。对每个像素点的像素值,用一个混沌实数序列值的小数点后某几位数字构造的密钥进行异合得到替代加密后的像素值。具体的替代变换过程为:假定图像大小为 $M\times N$,用 Lorenz 系统生成长度为 $L(L=M\times N)$的 $x、y、z$ 序列,随机选择 x,y,z 中的一个序列 r 作为密钥序列,取 r 的小数点后 7、8、9 三位数字组成正整数,将该正整数对 256 取模运算得到 1 字节的无符号整数 Intkey,将 Intkey 作为像素值的加密密钥。采用 1 字节密钥和 1 字节明文进行二进制逐比特位异或运算进行加密。重复以上步骤直到置乱图像的每个像素点都进行了像素值的替代变换。最后得到经过置乱和替代变换后的最终加密图像。

3　实验结果与分析

采用 Matlab7.0 平台,取 256×256 Lena 灰度图像进行实验,猫映射混沌系统的初值分别为:$[(x_0,y_0)]=[0,1]$,生成两个长度为 34 000 的序列,去掉前面 2 464 个点得到的两个序列 $\{x(i),y(i),i=1,2,\cdots,32\ 768\}$用于图像像素位置的置乱加密;Lorenz 系统的参数取 $\sigma=10,r=28,b=8/3$,初值 $x_0=1.184\ 0,y_0=1.362\ 7,z_0=1.251\ 9$,积分步长取 0.001,得出的实验结果如下:

(1)加密效果分析



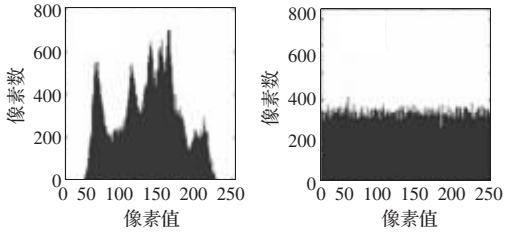
(a)原始图像　(b)加密后的图像　(c)正确解密后的图像　(d)x_0 误差 10^{-15} 解密后的图像

图 1　加密效果图

由图 1(b)可知,解密后图像面目全非,分辨不出图像的原始面貌,正确解密后的图像(c)与原图像完全相同,而在初值误差为 10^{-15} 时解密不出原始图像。可知,该算法加密效果良好,并具有很强的初值敏感性。

(2)直方图分析

由图 2 可知加密前像素值分布不均匀,加密后像素点均匀分布在[0,255]的区间中。可知,该算法具有较强的抵御统计分析攻击能力。



(a)原始图像直方图　(b)加密后图像直方图

图 2　加密前后直方图

(3)相关性分析

为了检验明文图像和密文图像相邻像素的相关性,从图像中随机选取全部水平方向相邻像素对、全部垂直方向相邻像素对和部分对角方向相邻像素对,用如下公式定量计算相邻像素的相关系数:

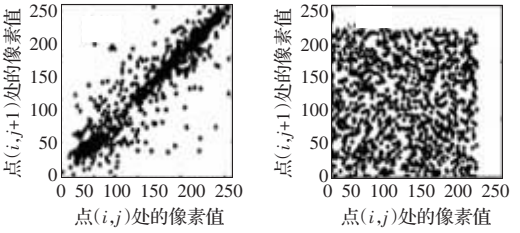
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{4}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2 \tag{5}$$

$$Conv(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][y_i-E(y)] \tag{6}$$

$$\gamma_{xy}=\frac{Conv(x,y)}{y\sqrt{D(x)}\sqrt{D(y)}} \tag{7}$$

其中,x 和 y 分别表图像中相邻两个像素的像素值,γ_{xy} 为图像相邻两个像素的相关系数。表 1 列出了按水平、垂直、对角三个方向的相关数。图 3 描述了明文和密文水平方向相邻像素的相关性。由结果可知,原始明文图像的相邻像素是高度相关的,相关系数接近于 1。而加密图像的相邻像素相关系数接近于 0,相邻像素已基本不相关,说明明文的统计特征已被扩散到随机的密文中,能够有效地抵御统计攻击。



(a)原始图像相关性　(b)加密后图像相关性

图 3　加密前后相关性分析

表 1　明文和密文相邻像素的相关性

方向	明文	密文
水平	0.965 6	−0.005 1
垂直	0.966 2	−0.002 6
对角	0.915 6	−0.002 7

(4)执行效率分析

算法采用 Matlab7.0,Intel Core 2 Duo E4600 的 CPU,2 G 内存,Windows XP 操作系统平台中实现时,算法所用时间如表 2 所示。

表 2　加密解密时间表

图像大小(像素)	加密时间/s	解密时间/s
128×128	0.12	0.12
256×256	0.21	0.21
512×512	1.08	1.08

4　结论

提出了基于广义猫映射及 Lorenz 高维混沌系统组合的图像加密算法。算法具有以下主要优点:(1)像素的位置置换和像素值的替代变换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。(2)以两种高维混

(下转 107 页)