基于二维超混沌序列的图象加密算法

李雄军 彭建华 徐 宁 周仁锋 李利辉 陈泽帆 冯祖添
(深圳大学理学院应用物理系,深圳 518060)

摘 要 图象加密日益受到重视,许多加密算法被提出,其中一维混沌加密算法由于利用了混沌序列的良好复杂性、伪随机性和对初值的敏感特性而具有较好的加密性能,但与其他方法比较,其最大的缺陷是密钥空间太小. 为此研究了一种基于二维超混沌系统的图象加密新方法,设计了若干个形式简单的二维超混沌模型,把它们生成的混沌序列变换成加密因子序列,采用纵横两重逐位模 2 加运算来加密、解密图象. 实验研究表明,该方法加密速度快,密钥空间增大,抗破译强度提高,并有一定抗破损鲁棒性.

关键词 计算机图象处理(520·6040) 图象加密 超混沌 二维离散系统 Lyapunov 指数
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2003)10-1172-06

Image Encryption Algorithm Based on 2D Hyperchaotic Sequences

LI Xiong-jun, PENG Jian-hua, XU Ning, ZHOU Ren-feng
LI Li-hui, CHEN Ze-fan, FENG Zu-tian
(*Department of Applied Physics, School of Science, Shenzhen University, Shenzhen* 518060)

Abstract The security of digital images attracts much attention recently, and many image encryption methods have been proposed. Among them, the 1D chaotic image encryption method was reported with appropriate performances by using the appropriate complexity and pseudo-randomness and extreme parameter sensitivity of chaotic sequences but with smaller key space as its serious drawback compared with others. So a new image encryption algorithm based on hyperchaotic sequences is studied. Several fast simple 2D hyperchaotic systems are given and studied. A linear approach of mapping from the model parameters to the key is proposed in order to make full use of the key space and keep the correspondency between the key and the model parameters used for encryption. The chaotic sequences generated by these models are mapped into the encrypt sequences, then the image is encrypted by the encrypt sequences by using two directional XOR horizontally and vertically. Experimental results show that this method is effecient, witch can provide faster encryption and larger key space and stronger anti-decryption-ability and rubustness to local breakage compared with the 1-D chaotic image encryption.

Keywords Computer image processing, Image encryption, hyperchaos, two dimensional discrete systems, Lyapunov exponents

0 引 言

混沌运动是非线性确定性系统的一种内在随机过程的表现,混沌运动轨道中嵌入了无数的不稳定轨道,这些不稳定轨道处处稠密,并与混沌运动共存. 近年来,混沌现象的应用研究越来越受到人们的重视,其中混沌保密通讯技术的研究已经成为国内外的热门课题[1]. 混沌保密通讯技术主要采用混沌同步通讯和直接利用混沌信号加密两种方法[2]. 基于混沌系统的直接加密过程主要是利用由混沌系统迭代产生的序列,通过某种变换变为加密变换的因子序列来对图象进行加密和解密,由于混沌序列提供了良好的复杂性和类随机性,具有很高的保密安全性. 目前广泛应用于加密的混沌模型是一维离散系统(如 Logistic 映射),其有着形式简单、产生混沌时序时间短等优点,但其缺陷是密钥空间太小[3]. 为此,本文提出了一种基于二维超混沌系统的图象加

基金项目:教育部高等学校骨干教师资助计划项目(200065);教育部科学技术研究重点项目(200000042)
收稿日期:2002-11-05;改回日期:2003-04-21

密新方法，它既能扩大密钥空间，又进一步提高了加密系统的抗破译强度.

1　混沌序列与二维混沌离散系统模型

混沌(chaos)定义为：设 X 为一个度量空间，$f:X\to X$ 称为在 X 上是混沌的，如果

(1) f 对初始条件的敏感依赖性：如存在 $\delta>0$ 对任何 $x\in X$ 和 x 的任何邻域 N，存在 $y\in N$ 和自然数 $n\geq 0$，使得 $d(f^n(x),f^n(y))>\delta$.

(2) f 是拓扑传递的：如对任何一对开集 U，$V\subset X$，存在 $k>0$，使得 $f^k(U)\cap V\neq\Phi$.

(3) 周期点在 V 中稠密.

Lyapunov 指数(简称李氏指数)是刻画非线性系统混沌特性的有效方法之一，李氏指数的个数与系统状态空间的维数 n 相同，若只有一个李氏指数大于零，则系统是混沌的；若至少有两个李氏指数大于零，则系统是超混沌的. 大于零的李氏指数个数愈多，系统不稳定的程度愈高[4]. 一般来说，系统的状态量个数越多(如高维系统，对离散系统来说，$n>2$)，它可能出现不稳定的程度会越高.

目前被广泛研究的一维混沌系统是 Logistic 映射，即

$$x_{k+1}=\mu x_k(1-x_k) \tag{1}$$

其中，$0\leq\mu\leq 4$ 称为分枝参数，$x_k\in(0,1)$. 混沌动力系统的研究工作指出，当 $3.569\,945\,6\cdots<\mu\leq 4.000\,0$ 时，Logistic 映射工作处于混沌态. 也就是说，由初始条件 x_0 在 Logistic 映射的作用下所产生的序列 $\{x_k;k=0,1,2,3\cdots\}$ 是非周期的、不收敛的并对初始值非常敏感的[5].

Logistic 映射的另一种形式为

$$x_{k+1}=1-\lambda x_k^2 \tag{2}$$

其中，$\lambda\in[0,2]$，x_k 的定义区间是 $(-1,1)$. 当 $1.401\,15<\lambda<2.000\,00$ 时，Logistic 映射工作处于混沌态.

不失一般性，二维混沌离散系统有如下形式[6]

$$\begin{cases}x_{n+1}=f_1(x_n,y_n)\\ y_{n+1}=f_2(x_n,y_n)\end{cases} \tag{3}$$

其中

$$\begin{cases}f_1(x_n,y_n)=a_1+a_2x_n+a_3x_n^2+a_4y_n+a_5y_n^2+a_6x_ny_n\\ f_2(x_n,y_n)=a_7+a_8x_n+a_9x_n^2+a_{10}y_n+a_{11}y_n^2+a_{12}x_ny_n\end{cases}$$

式中，$a_i(i=1,2,\cdots,12)$ 均为待定常系数.

采用高维系统产生超混沌，由于系统较之低维情况复杂，产生超混沌时序的时间增长，将有可能直接影响保密通讯实时性的要求，因此，如何在系统状态变量个数尽可能少而正性李氏指数又尽可能多的条件下，寻找到非线性形式简单的系统，是十分实际而又有意义的工作[4]. 为了寻找简单形式的二维离散超混沌系统，需进一步简化(3)式，使部分非线性项前的系数为零，然后通过计算该系统的李氏指数，即有两个或两个以上大于零的李氏指数，可认为该系统是超混沌特性的二维离散系统. 通过计算，最后得到一些形式简单且具有超混沌特性的二维离散系统如表 1 所示.

表 1　形式简单且具有超混沌特性的二维离散系统

系统序号	二维离散方程	参数值	Lyapunov 指数
1	$\begin{cases}x_{n+1}=a_4y_n+a_5y_n^2\\ y_{n+1}=a_8x_n+a_{10}y_n\end{cases}$	$a_4=1.55$ $a_5=-1.3$ $a_8=-1.1$ $a_{10}=0.1$	0.738 0.166
2	$\begin{cases}x_{n+1}=a_5y_n^2\\ y_{n+1}=a_7+a_8x_n+a_{10}y_n\end{cases}$	$a_5=1.3$ $a_7=-1.05$ $a_8=1.15$ $a_{10}=-0.2$	0.711 0.046
3	$\begin{cases}x_{n+1}=a_2x_n+a_4y_n\\ y_{n+1}=a_7+a_8x_n^2+a_{10}y_n\end{cases}$	$a_2=-0.95$ $a_4=1.55$ $a_7=-0.45$ $a_9=2.4$ $a_{10}=1.05$	0.302 0.240
4	$\begin{cases}x_{n+1}=a_4y_n+a_6x_ny_n\\ y_{n+1}=a_7+a_8x_n+a_{10}y_n\end{cases}$	$a_4=-0.95$ $a_6=-1.1$ $a_7=0.55$ $a_8=1.55$ $a_{10}=-1.8$	0.175 0.066

以离散系统 1 为例，用它生成数字图象加密的加密变换的因子序列. 先分析其简单分岔特性(如图 1，图 2 所示)，为选取合适的参数值和密钥空间做好准备. 假若 $a_5=-1.3$，$a_8=-1.1$，$a_{10}=0.1$ 先固定.

实验发现 $a_4=0.91$ 时，离散系统 1 进入准周期运动(图 3)，而 $a_4=1.66$ 时，该系统已经是超混沌态了(图 4)，同时可以计算出此时序列区间为

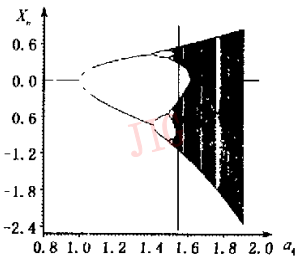


图 1　a_4 和 x_n 为参数的分岔图

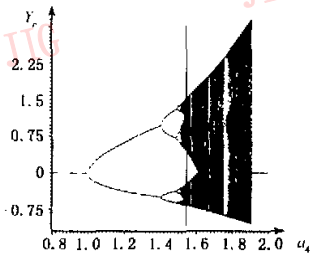


图 2 a_4 和 y_n 为参数的分岔图

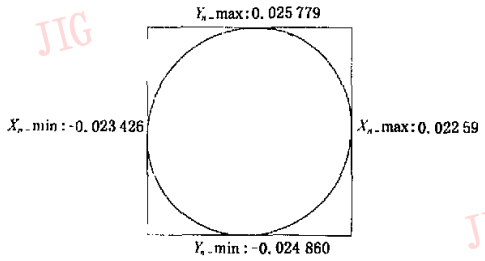


图 3 二维离散混沌方程的准周期运动

($a_4=0.91, a_5=-1.3, a_8=-1.1, a_{10}=0.1$)

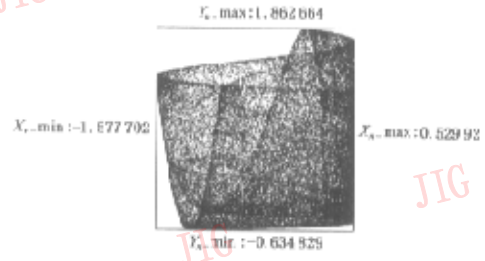


图 4 二维混沌吸引子

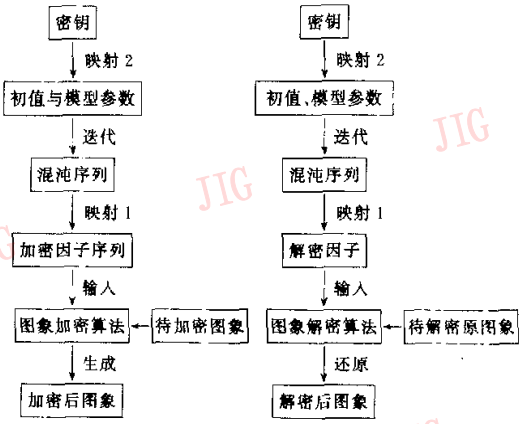
($a_4=1.66, a_5=-1.3, a_8=-1.1, a_{10}=0.1$)

$-1.577\,702<x_n<0.529\,923$; $-0.634\,822<y_n<1.862\,664$.

2 二维混沌系统应用于图象置乱加密

基于混沌序列图象加密和解密模型可以用图 5 表示. 显然,图象加密算法和对应的解密算法是需研究和解决的核心问题,除此之外,由混沌实数序列生成直接应用于加密变换的因子序列的变换(映射 1),以及密钥与用来决定密钥的初值和模型参数之间的映射 2 也是需要研究解决的问题.

映射 1 设计的原则是让加密因子序列尽量保持原混沌序列的伪随机性,同时适于后续加密算法的操作. 目前,常用的映射 1 大体上分为实数值序列、



(a) 加密系统模型 (b) 解密系统模型

图 5 混沌加密、解密系统模型

位序列和二值序列 3 种.

(1) 实数值序列,即$\{x_k; k=0,1,2,3\cdots\}$,是混沌映射的轨迹点所形成的序列. 显然不宜直接应用于加密图象,而且理论研究表明:这种无误差的平凡混沌加密方法是可破解的[7].

(2) 位序列:同样由实数值混沌序列得到,所不同的是,位序列是通过对$\{x_k; k=0,1,2,3\cdots\}$中的 x_k 改写为 L-bit 的浮点数形式得到的

$$|x_k|=0.b_1(x_k)b_2(x_k)\cdots b_i(x_k)\cdots b_L(x_k)$$

其中,$b_i(x_k)$是$|x_k|$的第 i 位. 所需序列即为$\{b_i(x_k); i=0,1,2,\cdots,L; k=0,1,2,3\cdots\}$. 显然该位序列 $b_i(x_k)$的取值范围是[0,9],不适合直接作用于 8bit 和 24bit 的图象数据.

(3) 二值序列,即将原混沌序列阈值化后生成的二值序列,混沌序列阈值化后,其混沌伪随机性损失较大,通过实验发现,加密后的图象轮廓依稀可见.

针对数字图象的特点,结合加密效果和效率指标要求,提出一种新的方法,即将混沌实数序列在其最大值和最小值之间,按 256 级等级线性映射,得到 8 位二进制序列,作为加密因子序列.

二维超混沌模型的多个参数和两个初始条件都可以设计为密钥. 由于采用的是私钥方式,为方便用户使用,一般来说,密钥空间的连续性是首先必须保障的,如是 8 位密码的话,密钥最好可以从 00000000～99999999 连续取值. 其次,从密钥到初值和(或)模型参数的映射 2 可以有多种形式,在此推荐分节线性变换方法,该方法既保证密钥与初值或参数的一一对应性和同步相异性(在一定计算精

度范围内），又充分利用了系统可能提供的密钥空间大小，更重要的是它可以有效地防止初值区间超出混沌迭代序列的区间而使密钥无效这种致命问题的出现.

以 18 位十进制密钥为例，它可被分为 3 节（长度可以相等或不等），3 节分别通过线性映射，映射为用于解密的初值 x_0, y_0，和模型参数 μ.

密钥 P：XXXXXX　XXXXXX　XXXXXX（每一位 X 的取值范围是 0 到 9）.

$x_0=k_1p_1+c_1; y_0=k_2p_2+c_2; \mu=k_3p_3+c_3$

基于纵横两重异或（模 2 加）运算的图象加密新方法，其优点是计算速度快，加密效果好，容易程序实现，可以抵御一定程度的攻击.

纵横两重异或加密、解密算法描述如下：

加密算法/过程为

（1）给定需要加密的原图象 $I=\{0\le f_k(i,j)\le 255$，若图象为彩色图象，$k=1,2,3$ 代表 3 种颜色分量；若图象为灰度图象，$k=1, i=0,1,2,\cdots,M-1; j=0,1,2,\cdots,N-1\}$ 和密钥 P，图象分辨率为 $M\times N$；

（2）由密钥 P 映射出混沌系统的初值和模型参数；

（3）生成二维混沌序列；

（4）由实数值混沌序列通过线性变换映射到 0～255 的整数序列作为加密因子序列；

（5）在横向上用生成的加密因子序列对原图象进行异或加密，对于彩色图象，每个像素的多个颜色分量可以采用同一加密因子序列或紧邻的加密因子序列加密；

（6）在纵向上用生成的加密因子序列对原图象进行异或加密；

（7）将加密后的图象在公共通道上传输；

（8）将密钥 P 在安全通道上传输.

解密算法/过程为

（1）从公共通道上得到加密图象；

（2）用从安全通道上得到的密钥 P；

（3）由密钥 P 映射出混沌系统的初值和模型参数；

（4）生成二维混沌序列；

（5）由实数值混沌序列通过线性变换映射到 0～255 的整数序列作为加密因子序列；

（6）在纵向上用生成的加密因子序列对原图象进行异或解密；

（7）在横向上用生成的加密因子序列对原图象进行异或解密；

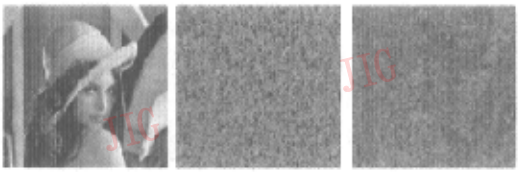
（8）生成恢复后的图象.

3　实验结果

上述加密解密算法用 Visual C++编程实现，分别对灰度图象和 24 位彩色图象加密和解密，并进行了测试. 实际计算中去掉了前5 137次暂态过程，选取离散系统中的初始条件 x_0 和 y_0 来产生密钥. 图 6～图 10 给出了以离散系统 1 为模型的实验结果.

(a) Lena 原图　(b) 混沌序列随机图　(c) 异或加密结果

图 6　X 方向混沌加密实验（密钥 11415923）



(a) Lena 原图　(b) 混沌序列随机图　(c) 异或加密结果

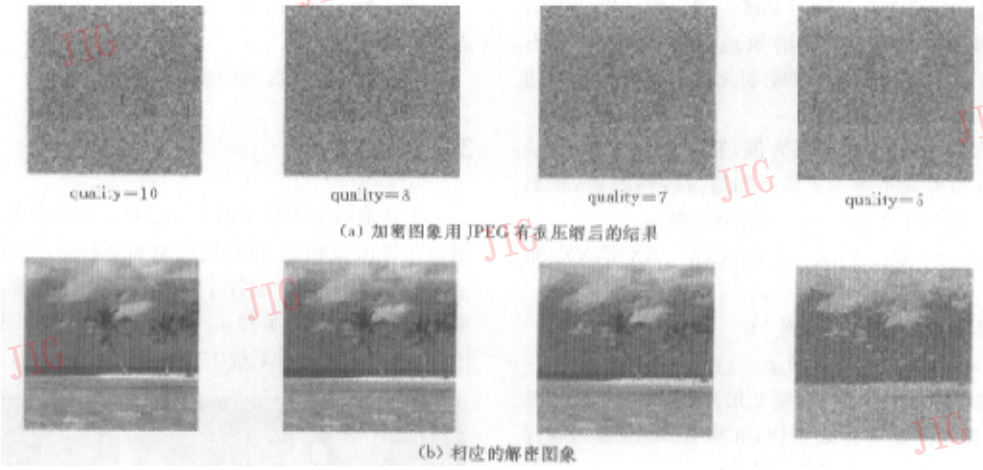
图 7　Y 方向混沌加密实验（密钥 11415926）

(a) 纵横两重异或加密结果（密钥 11415956）　(b) 正确密钥还原结果（密钥 11415923）　(c) 错误密钥还原结果（密钥 11415927）

图 8　纵横两重混沌加密实验

(a) 纵横两重加密结果局部破坏　(b) 还原结果

图 9　局部破损实验



(a) 加密图象用 JPEG 有损压缩后的结果

(b) 相应的解密图象

图 10 有损压缩实验

从实验测试结果可以看出:

(1) 对图象进行 X 或 Y 单个方向的混沌加密,如图 6、图 7 所示,可以看到:原图象的轮廓依稀可见,置乱效果欠佳.但纵横两重异或加密后,图象变得杂乱无章,置乱效果明显,有良好的保密性.

(2) 由于混沌系统对初始值的敏感性,当改变密钥 11415927(原密钥 11415926),不但不能恢复原图象,而且还原出的图象依旧很混乱,如图 8.

(3) 局部破损实验中对加密后的图象进行部分破损,还原后,可以看出:破损部分没有扩散,其余部分能正确地还原,如图 9 所示.

(4) 从表 2 的加密、解密时间来看,虽然二维超混沌系统比一维系统计算复杂,但加密的速度还是相当快的.

表 2 加密/解密时间对比表

	256×256×24bit	1 024×768×24bit
一维混沌加/解密	34	1 312
二维混沌加/解密	53	1 464

实验系统配置:CPU 奔龙 750;内存 128MB;主频 133MHZ;操作系统: Windows XP.

(5) 网络传输的需要,往往会对原图象进行有损压缩(如 JPEG),到达目的地后再将其转换为 BMP 格式,再去乱还原.如图 10 所示实验结果表明:压缩的品质因子 quality 大于 5 时,还原效果较好,当品质因子小于 5 时,去乱后的图象是不可用的.

4 结 论

对目前一维混沌序列用于加密时密钥空间小及平凡混沌加密易被破解等缺点做了改进,即采用二维超混沌模型;研究了从混沌序列到加密因子序列的映射方法和用混沌系统初值与模型参数来产生密钥的方法,提出了纵横两重模 2 加加密解密算法.设计的二维混沌模型继承了一维混沌模型的形式简单、生成速度快等优点,同时由于其超混沌态,抗破译强度进一步增强,其多个参数和两个初始条件都可以设计为密钥,使密钥空间大大扩展.实验结果证明,该算法具有较广泛的普适性,对灰度图象、彩色图象和压缩图象都适用.进一步需解决的是超混沌加密在网络视频保密通讯上应用的可行性、实时性与容错性问题.

参 考 文 献

1 Maniccam, Suchindran, Sanmuganathan. Image-video compression, encryption, and information hiding [D], State University of New York, Binghaminton, New York, USA, 2001.

2 Scott Hayes, Celso Crebogi, Edward Ott. Communicating with chaos[J]. Phys Rev Lett, 1993, 70(20): 3031~3034.

3 Josef Scharinger. Fast encryption of image data using chaotic Kolmogorov flows [A]. In: Proceedings of the Symposium on Electronic Imaging: Science and Technology-Storage and Retrieval for Image and Video Drabase V [C], San Jose, California, 1997, 3022: 278~289.

4 Wolf A, Swift J B, Swinney H L *et al*. Determing Lyapunov

exponents from a time series [J]. Physica D: Nonlinear Phenomena, 1985,16(3):285～317.
5 王宏，程磊，彭建华. 超混沌加密数字信号的应用[J]. 东北师大学报(自然科学版)，2001,33(3):31～35.
6 程丽，陶路，黄秋楠等. 构造具有超混沌特性的二维离散系统[J]. 东北师大学报(自然科学版)，2002,34(3):47～52.
7 高俊山，徐松源，孙百瑜等. 基于混沌理论的加密过程的研究[J]. 自动化技术与应用，2001,6:13～16.

李雄军　1966 年生，1995 年获华中理工大学工学博士学位，现为深圳大学理学院应用物理系副教授. 主要研究领域为图象处理、模式识别与人工智能、机器视觉.

彭建华　1955 年生，1985 年获华北师范大学理学硕士学位，现为深圳大学理学院应用物理系教授. 研究方向为非线性系统的混沌理论及应用.

徐　宁　1981 年生，2003 年于深圳大学理学院获理学学士学位. 研究兴趣包括图象加密、图象处理与模式识别.

周仁峰　1980 年生，深圳大学理学学士学位. 研究兴趣包括智能信息处理、数据库技术.

李利辉　1981 年生，深圳大学理学院应用物理系本科生. 研究兴趣包括智能信息处理、数据库技术.

陈泽帆　1981 年生，深圳大学理学院应用物理系本科生. 研究兴趣包括智能信息处理、算法.

冯祖添　1980 年，深圳大学理学院应用物理系本科生. 研究兴趣包括图象处理、计算机应用.