基于新的超混沌系统的图像加密方案

卢辉斌 孙 艳

(燕山大学信息科学与工程学院 秦皇岛 066004)

摘 要 提出了一个新的超混沌系统,分析了新系统的混沌吸引子相图、平衡点及其性质、Lyapunov指数等非线性动力学特性,并用该超混沌系统对图像进行加密研究。给出了一种新的基于四维超混沌系统的图像加密算法。实验结果及安全性分析表明,该算法具有较强的抵御穷举攻击、统计攻击、已知明文攻击能力,因而具有较高的安全性。

关键词 超混沌系统,混沌序列,Lyapunov指数,图像加密

中图法分类号 TP309 **文献标识码** A

Image Encryption Scheme Based on Novel Hyperchaotic System

LU Hui-bin SUN Yan

(College of Information Science and Engineering, Yanshan University, Qinhuangdao, 066004, China)

Abstract Proposed a new hyperchaotic system, analyzed the new system, the phase diagram of the chaptic attractor, and the nature of the equilibrium point, Lyapunov exponent, nonlinear dynamics properties and so on, proposed a novel image encryption scheme based on a four dimensional hyperchaotic system. The experimental results and security analysis show that the new scheme has stronger resistance for the exhaustion attack, count attack and known-plaintext attack, and it is of high security.

Keywords Hyperschaotic system, Chaotic sequences, Lyapunov exponent, Image encryption

1 引言

混沌作为一种特有非线性现象,具有良好的伪随机特性、轨道的不可预测性、对初始状态及结构参数的极端敏感性、迭代的不重复性等一系列优良特性[1,6],由于越来越广泛使用的图像、多媒体信息,数据量大,冗余度高,已给传统密码提出了挑战,混沌信号天然的随机性和隐蔽性非常适用于保密通信。

众所周知,一个好的加密算法应该对密钥极其敏感,密钥空间足够大,以抵御穷举攻击。虽然一维、二维混沌映射具有形式简单、运行效率高等优点[2],但低维混沌存在密钥空间小、安全性不高的缺点。高维超混沌具有更高的复杂性、随机性和更好的不可预测性,能更有效地抵御相空间重构等破译方法的进攻,保密性强,算法实现简单,密钥空间大[8]。与混沌系统相比,超混沌系统有更多正的李雅普诺夫指数、更加复杂和难以预测的动力学特性。正的李雅普诺夫指数越多,系统轨道不稳定方向越多,系统随机性越强,其抗破译能力越高[3]。

本文首先构造了一个新超混沌系统,并提出了基于该超混沌映射的图像加密新方案。四维映射的参数和系统变量的增大使密钥量也随之增加,从而可有效地抵御穷举攻击;加密图像像素值分布随机,具有较高的安全性。

2 新超混沌系统

新的超混沌系统的动力学方程如下:

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=bx-xz+w\\ \dot{z}=-cz+dx^2\\ \dot{w}=-ry\end{cases} \tag{1}$$

要产生超混沌吸引子,必须满足以下几个条件:首先动力学方程应该有耗散性,方程的维数不小于4;系统至少有两个增强不稳定因素的方程,同时这两个方程中至少有一个含非线性项,且平衡点为不稳定的。取系统参数 $a=10, b=45, c=2.5, d=4$,r 为后来引进的参数,这里设 $r=5$。

2.1 基本动力学分析

2.1.1 耗散性和吸引子的存在性

由于

$$\nabla V=\frac{\partial\dot{x}}{\partial x}+\frac{\partial\dot{y}}{\partial y}+\frac{\partial\dot{z}}{\partial z}+\frac{\partial\dot{w}}{\partial w}=-a-c=-55<0 \tag{2}$$

系统(1)是耗散的,且以如下指数形式收敛:

$$\frac{dv}{dt}=e^{-(a+c)} \tag{3}$$

即体积元 v_0 在 t 时刻收缩为体积元 $v_0e^{-(a+c)t}$。这意味着,当 $t\to\infty$ 时,包含系统轨迹的每个体积元以指数率 e^{-a-c} 收缩到零。因此,所有系统轨迹最终会被限制在一个体积为零的集合上,且它渐进运动固定在一个吸引子上。

2.1.2 平衡点及稳定性

令式(1)的右边等于0:

到稿日期:2010-07-06 返修日期:2010-10-12 本文受河北省教育厅基金(2007493)资助。

卢辉斌(1964-),男,博士后,教授,主要研究方向为网络信息安全与保密通信、计算机网络拥塞控制技术、交换技术及图像处理,E-mail:yjsbl@ysu.edu.cn;孙 艳(1983-),女,硕士生,主要研究方向为混沌保密通信、信息安全,E-mail:sunyan338@126.com(通信作者)。

$$\begin{cases} a(y-x)=0 \\ bx-xz+w=0 \\ -cz+dx^2=0 \\ -ry=0 \end{cases} \tag{4}$$

显然系统(1)存在一个平衡点 $s_0=(0,0,0)$。在平衡点 s_0，对系统(1)进行线性化，得其 jacobian 矩阵：

$$J_0=\begin{bmatrix} -a & a & 0 & 0 \\ b-z & 0 & -x & 1 \\ 2dx & 0 & -c & 0 \\ 0 & -r & 0 & 0 \end{bmatrix}=\begin{bmatrix} -a & a & 0 & 0 \\ b & 0 & 0 & 1 \\ 0 & 0 & -c & 0 \\ 0 & -r & 0 & 0 \end{bmatrix}$$

为了求平衡点 s_0 相应的特征根，令 $\det(J_0-\lambda I)=0$，得相应的特征根为 $\lambda_{10}=-26.7226$，$\lambda_{20}=16.6099$，$\lambda_{30}=0.1126$，$\lambda_{40}=-2.5000$，4 个特征值皆为实数，这里 λ_{20}，λ_{30} 为正实根，λ_{10}，λ_{40} 为负实根。因此，平衡点 s_0 为不稳定的鞍焦点。

2.2 Lyapunov 指数和 Lyapunov 维数

当参数为 $a=10$，$b=45$，$c=2.5$，$d=4$，$r=5$ 时，系统的 Lyapunov 指数 $\lambda_1=1.7365$，$\lambda_2=0.0466$，$\lambda_3=-0.0049$，$\lambda_4=-14.2675$，系统有两个正的 Lyapunov 指数，式(1)为超混沌系统。此超混沌系统的 Lyapunov 维数为：

$$D_L=j+\frac{1}{|\lambda_{j+1}|}\sum_{i=1}^{j}\lambda_i=3+\frac{(\lambda_1+\lambda_2+\lambda_3)}{|\lambda_4|}=3.125 \tag{5}$$

由此可见，这个新系统的 Lyapunov 维数是分数维数，从而验证了该系统为超混沌系统[7]。

2.3 混沌吸引子

当系统参数 $a=10$，$b=45$，$c=2.5$，$d=4$，$r=5$ 时，系统(1)存在一个典型的混沌吸引子。采用四阶 Runge-Kutta 离散化算法，迭代 10000 次，取后面 9900 个数据得到混沌吸引子相图，如图 1 所示。由图 1 可知，系统的混沌吸引子轨线在特定的吸引域内具有遍历性，对应吸引子在各平面的投影。

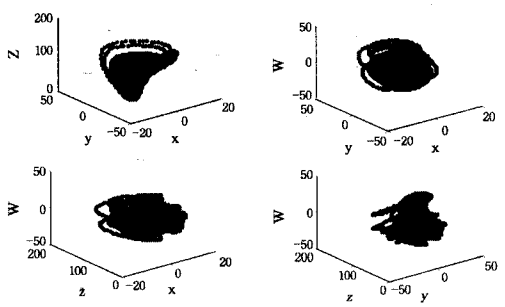


图 1 系统(1)的超混沌吸引子

该四维超混沌系统生成的混沌序列有如下特点：①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；②是处理系统输出的实数值混沌序列，可产生单变量或多变量组合的加密混沌序列，使加密序列的设计非常灵活；③是系统的 4 个初始值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远远高于低维混沌系统。

3 加密算法设计

3.1 像素位置置乱

为了扰乱图像相邻像素间高度相关性，利用置乱矩阵来置乱原图像像素位置。这样，原图像的全部像素将被随机均匀地置乱到密文图像的整个像素空间。

设原始图像大小为 $M\times N$，$P(i,j)$，$i=0,1,\cdots,M-1$，$j=0,1,\cdots,N-1$，表示图像的像素灰度值。采用如下方法对图像像素位置进行置乱：

Step1 给定初始值超混沌系统(1)在四阶龙格一库塔法迭代 N_0 次生成 4 个混沌序列$\{x_1(k),x_2(k),x_3(k),x_4(k)|k=0,1,2,\cdots\}$，并舍弃每个序列的前 10000 个值，将后面的值作为混沌序列。

Step2 对混沌序列 $x_1(k)$，$x_3(k)$进行如下预处理：

$$\begin{cases} x_1(k)=abs(x_1(k))-fix(x_1(k)) \\ x_3(k)=abs(x_3(k))-fix(x_3(k)) \end{cases} \tag{6}$$

Step3 将 Step2 中产生的混沌序列排序，组成两个新序列，原混沌序列中的两个值在新序列中位置编号组成的序列，将这两个序列作为图像数据矩阵的行序列和列序列，从而实现对原图像位置的置乱。

置乱破坏了原图像相邻像素点相关性，但是图像的灰度直方图并没改变，因而安全性不够高，很难抵御已知明文攻击，需要对预处理后的图像做进一步加密。

3.2 图像像素值扩散

使用超混沌系统产生的混沌序列对置乱后图像进行加密，对于每个像素点构造一个实数序列值的密钥。这种改变基于超混沌系统的像素灰度值的步骤如下：

Step1 由超混沌系统产生的 4 个混沌序列组成正整数，将该正整数对 256 取模，得到 1 字节的加密密钥来加密图像，公式如下：

$$x_i=\mathrm{mod}(fix((abs(x_i)-floor(abs(x_i)))\times 10^{15}),256),\quad i=1,2,3,4 \tag{7}$$

式中，abs 表示取 x_i 绝对值，$floor$ 表示取小于或等于 x_i 的整数，mod 表示取余运算。

Step2 由下面公式产生$\hat{x}_0$：

$$\hat{x}_0=\mathrm{mod}(x_4,4) \tag{8}$$

式中，$\hat{x}_0\in[0,3]$。根据$\hat{x}_0$选择加密混沌序列。若$\hat{x}_0=0$，用(x_1,x_2,x_3)进行异或加密；若$\hat{x}_0=1$，用(x_2,x_3,x_4)进行异或加密；若$\hat{x}_0=2$，用(x_1,x_2,x_4)进行异或加密；若$\hat{x}_0=3$，用(x_1,x_3,x_4)进行异或加密。

Step3 每次对图像中 3 个像素值进行异或运算，再与前一个密文图像进行异或，直到完成所有的像素点加密为止。初始值 $C(0)=100$，计算公式如下：

$$\begin{cases} C(3\times i+1)=P(i+1)\oplus x_1\oplus C(3\times i) \\ C(3\times i+2)=P(3\times i+2)\oplus x_2\oplus C(3\times i+1) \\ C(3\times i+3)=P(3\times i+3)\oplus x_3\oplus C(3\times i+2) \end{cases} \tag{9}$$

式中，$i=0,2,\cdots,[(M*N)/3]-1$，$P(i)$和 $C(i)$分别代表了置乱后的图像和密文图像像素灰度值。⊕表示异或运算。

重复以上步骤，直至每个像素点都进行了像素值替代变换，最终得到置乱和替代变换后的加密图像。

此方案中加密序列的选取与新超混沌系统相关，这样混沌序列的产生依赖于密钥，混沌序列的选择对混沌系统也是敏感的，这就能有效地增强算法的安全性。从替代变换算法看，由于对图像的每一个像素点都采用了不同的替代加密密钥，因此符合香农的“一次一密”加密原则，故算法具有抵抗强力攻击的安全性。

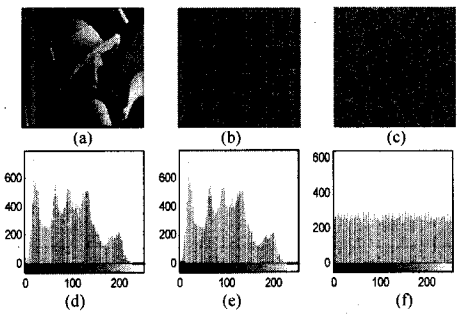
解密是加密的逆过程。加密过程是先置乱后替换。解密是先对密文图像像素值反替代，然后对反替代后图像像素进行位置反置乱，即可得到解密图像。

4 实验结果及分析

选用大小为256×256、灰度为256色的位Lena.bmp(图2(a))作为实验图片。一个好的加密算法应该能够抵御各种已知攻击,同时对加密密钥敏感,密钥空间足够大,以抵御穷举攻击。下面对加密算法进行安全性分析。

4.1 灰度直方图分析

从图2(a)－图2(f)中可以看出,置乱后图像的灰度直方图没发生改变,即图2(d)和图2(e)相同。经过本文加密,灰度直方图发生显著变化,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,本算法具有较强的抵御统计分析攻击能力。



(a)原始图像;(b)置乱后图像;(c)加密后图像

(d)原图灰度直方图;(e)置乱后灰度直方图;(f) 密文灰度直方图

图2 基于超混沌图像加密仿真图

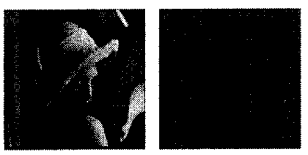
4.2 密钥空间分析和执行效率分析

在本算法中,超混沌映射的4个初始值和参数 r 均可用来作为密钥。若设置精度为 10^{-14},密钥空间超过 10^{70},同时超混沌系统初始迭代次数也可作为密钥,这样密钥空间就足以抵御各种攻击。在硬件环境为matlab7.4仿真平台,AMD Athlon(tm) 64 X2 Dual Core Processor 5600的CPU,1.75G内存,Windows XP操作系统平台中实现时,加密256×256图像所用的时间约0.82s,表明时间开销小。

4.3 密钥敏感性实验

密钥敏感性分析也就是密钥的微小变化将最终导致密文的显著变化。该特性有助于抵抗唯明文攻击[12]。混沌加密的安全性在于它的初始值敏感性,即攻击者用与初始值很相近的一个数值进行破解,也不能恢复出原始的图像。

图3为解密仿真的试验结果。图3(a)－图3(b)为初值敏感性实验,其中初始值 $x_1(0)=1.2, x_2(0)=0.3, x_3(0)=0.4, x_4(0)=0.5$,迭代次数 $N_0=2000$。图3(a)是正确解密后的图像,图3(b)是其余初始值不变 $x_1(0)=1.200000000001$ 时的解密图像,正确解密后的图3(a)与原图像完全相同,而初始密钥细微的差别都不能正确解密出原始图像。由此可知本加密算法对密钥非常敏感,加密效果良好,具有很强的初值敏感性。



(a) 正确解密后图像 (b) 错误解密图像

图3 解密图像

4.4 相邻像素点间的相关性分析

通过比较明文和密文图像相邻像素的相关性,可以考察算法对图像置乱的程度[5]。本文从明文图像和密文图像中随机选取3000对水平相邻像素对、垂直相邻像素对和对角相邻像素对,利用以下公式进行计算:

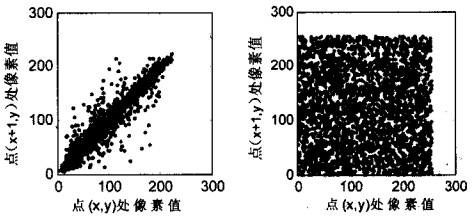
$$E(x_i)=\frac{1}{N}\sum_{i=1}^{N}x_i$$

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

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x_i))(y_i-E(y_i))$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

式中,x 和 y 表示随机选取的这3000对相邻像素的灰度值。测试结果如表1所列,图4显示了原始图像和加密后图像相邻像素点间的相关性。



(a) 原图垂直方向相关性 (b) 密文垂直方向相关性

图4 原始图像和密文图像垂直方向相关性分析

表1 明、密文像素相关性对比

方向	明文灰度值相关性	密文灰度值相关性
水平方向	0.9331	0.0064
垂直方向	0.9675	0.0084
对角方向	0.9239	0.0107

可以看出,明文图像相邻像素是高度相关的,相关系数接近1。而加密图像的相邻像素相关系数接近0,相邻像素间相关性明显减小,此时明文的统计特性已被扩散到随机的密文中,可以有效地抵御统计攻击。同时,与文献[10]中混沌系统相比,超混沌系统有更大的密钥空间。

结束语 本文基于新超混沌系统完成了对明文图像的置乱和像素的灰度值的替换与扩散,每一次迭代采用不同的加密密钥,经仿真分析,本文方案有效地克服了低维混沌系统不能抵御相空间重构攻击的缺点,拥有很大的密钥空间,具有抵御穷举攻击的能力。超混沌系统具有复杂的非线性混沌行为,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。安全性分析显示,加密算法效果良好,速度块,适用于图像加密以及实时加密传输[3],在信息安全领域有潜在的应用价值。

参 考 文 献

[1] 于万波.混沌的计算实验与分析[M].北京:科学出版社,2008:10-39

[2] Elnashaie S E E H, Abasha M E. On the chaotic behaviour of forced fluidized bed catalytic reactors [J]. Chaos, Solitons &Fractals, 1995, 5(5): 797-831

[3] 潘勃,冯金富,陶茜,等.基于超混沌映射和加法模运算的图像保密通信方案 [J].计算机科学,2009,36(8):273-275

[4] 关新平,范正平,陈彩莲,等.混沌控制及其在保密通信中的应用[M].北京:国防工业出版社,2002:16-21

[5] 石熙,张伟.基于广义猫影射和加法模运算的快速图像加密系统[J].计算机科学,2008,35(6):190-192

[6] 吕金虎,陆君安,陈士华.混沌时间序列分析及其应用[M].武汉

大学出版社,2002:72-92
[7] 刘凌,苏燕辰,刘崇新. 新三维混沌系统及其电路仿真实验[J]. 物理学报,2007,56(4):1966-1970
[8] Pareek N K, Vinod P, Sud K K. Image encryption using chaotic logistic maps[J]. Image and Vision Computing, 2006, 24 (9): 926-934
[9] Gao Tie-gang, Chen Zeng-qiang. A new image encryption algorithm based on hyper-chaos[J]. Physics Letters A, 2008, 372 (1):394-400
[10] Zhang Linhua, Liao Xiaofeng, Wang Xuebing. An image encryprion approach based on chaotic maps[J]. Chaos, Solitions & Frsctals, 2005, 24(1):759-765
[11] Gao T, Chen Z. Image encryption based on a new total shuffling algorithm[J]. Chaos, Solitons & Fractals, 2008, 38(1):213-220
[12] 郭建胜,沈林章,张锋. 基于混沌序列的图像加密算法的安全性分析[J]. 计算机工程,2008,34(8):12-15

(上接第 141 页)

FIN 标志位为 1,可以作为基于 TCP 协议的应用层会话的结束标志);还原策略用以确定对该类会话数据的分析以及还原的方法,如数据包的的长度、偏移量等。对于不同的协议,其使用的会话标识会有所区别。

· 会话信息结构

会话信息结构用于保存会话的相关信息,我们可以设计类似如下的一个结构体来存储之。

```
Struct SSessionDetail{
    char * m_SrcIP; //源 IP
    char * m_DstIP; //目的 IP
    long m_SrcPort; //源端口
    long m_DstPort; //目的端口
    long long m _FirstDataTime;
      //第一个包收到时间
    SDataQueue * m_pDataQueueFirst;
      //保存的数据包链表头指针
    …
};
```

在上述的会话状态结构中,SDataQueue 是一个用于保存本连接收到的有效数据包的队列。其数据结构为:

```
Struct SDataQueue{
    void * pData;
    int offset;
    int len;
    SDataQueue * p_Next;
    …
};
```

3.2.3 实验结果与分析

实验环境:根据架设 FTP 服务器,并将服务器部署到校园网网络核心,通过交换机端口镜像技术将与服务器相连端口的流量镜像到与 IDS 相连的端口上,这样 IDS 系统就能捕获出入 B 服务器的网络数据包。实验环境网络拓扑如图 4 所示。

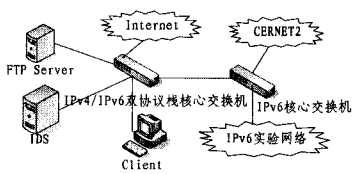


图 4 IPv4/IPv6 双协议栈网络拓扑图

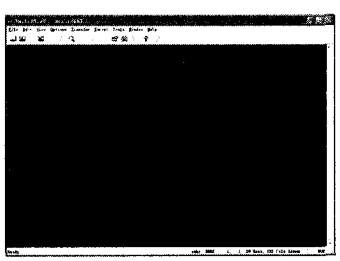


图 5 IDS 系统对 FTP 的审计结果截图

应用上述设计的算法,验证对 FTP 协议的审计。我们先从 FTP 客户端访问 FTP 服务器,然后输入一些命令,最后断开连接退出。IDS 系统审计截图如图 5 所示。客户端的操作命令与审计结果对比如表 1 所列。

表 1

FTP 客户端操作的命令	IDS 审计记录(被转成 FTP 的标准命令)	FTP 命令功能说明
root	USER root	登录账号
“ ”	PASS “”	登录密码,这里密码为空格
pwd	XPWD	显示当前路径
ls	NLST	显示当前路径下的所有文件
put abc. txt	STOR abc. txt	向服务端上传“abc. txt”
by	QUIT	断开连接

可以看出,FTP 客户端所有的操作命令都被审计出来了,说明基于设计的算法是正确有效的。

结束语 本入侵检测模型结合使用协议分析技术与网络审计技术,并对有关算法做改进,是本文的创新点。目前基于实验环境以及研究时间有限,并且基于 IPv4、IPv6 的应用服务在应用层使用相同的协议,因此我们只在 IPv4 下对 FTP 协议进行审计实验。今后的工作是在 IPv6 环境下进行有关实验,从而改进并验证本入侵检测系统对其他应用层协议的审计功能等。

参 考 文 献

[1] 庄绪春,孟相如,韩仲祥. 高速网络环境中入侵检测技术探讨[J]. 信息与电子工程,2006,4(4):288-291
[2] 王艳秋,赵昭灵,兰巨龙. 一种基于 IPv6 的网络入侵检测系统[J]. 计算机应用研究,2007(2):142-144,147
[3] 於时才,安凌鹏. 协议分析与深度包检测相结合的入侵防御系统信息安全[J]. 微计算机信息,2009,21:67-69
[4] Richard S W. TCP/IP 详解——卷 1:协议[M]. 北京:机械工业出版社,2000
[5] 张涛. 浅谈 IPv6 环境下的入侵检测[J]. 信息科学,2010,8:63
[6] 王强,王磊,魏光村. IPv4/IPv6 过渡阶段网络安全工具的设计与实现[J]. 计算机工程,2005,31(13):134-136
[7] 甘勇,吕国宁,马芳,等. 基于动态规则的 IPv6 入侵检测系统研究[J]. 信息安全,2008,24(4-3):78-80
[8] 贾新宇,肖玮基. 于入侵检测的校园网安全防御体系的研究[J]. 电脑知识与技术,2010,6(9)
[9] 许超,钱俊,史美林. 用于入侵检测数据集评测的 SMTP 流量模拟[J]. 计算机工程与设计,2006,27(12):2124-2127
[10] 刘海峰,卿斯汉,蒙杨,等. 一种基于审计的入侵检测模型及其实现机制[J]. 电子学报,2002,30(8)
[11] Anagnostakis K G, et al. E2xB: A domain-specific string matching algorithm for intrusion detection[C]// Proceedings of the 18th IFIP International Information Security Conference (SEC 2003). May 2003
[12] 张晨,王晓东. 基于支持向量机的网络入侵异常检测[J]. 重庆工学院学报:自然科学版,2007,21(12):119-121