DOI:10.13718/j.cnki.xsxb.2017.07.010

基于超混沌数学理论的图像加密方法研究①

陈 敏, 关英子

黄淮学院 数学与统计学院,河南 驻马店 463000

摘要:界定了混沌的概念,依据 Lypunov 指数构建了混沌系统判别方法. 深入剖析了 Lorenz 混沌系统数学模型、吸引子特征,进而构建了四维 Lorenz 混沌系统,即 Lorenz 超混沌系统. 相比于 Lorenz 混沌系统,Lorenz 超混沌系统非线性更强、运行轨迹更加随机,适用于图像加密. 实验结果表明,基于 Lorenz 超混沌系统构建的图像加密方法,加密结果中像素均匀置乱,三向相关性低.

关 键 词:混沌理论;Lorenz 混沌系统;超混沌系统;图像加密

中图分类号:O29 **文献标志码**:A **文章编号**:1000-5471(2017)07-0063-05

混沌一词最早出现于古希腊的物理学界,用于形容宇宙还没有形成以前的混乱形态[1]. 宇宙的形成和逐步成长,正是从混沌形态逐步发展成为有规律、有秩序的形态[2]. 近代自然科学技术兴起以后,数学家将各种有规律、有秩序的现象建立起对应的数学模型和数学公式,从而推动了数学理论在各个领域的应用[3-4]. 进入 20 世纪下半叶,数学家开始尝试对自然界的一些混沌现象进行数学抽象,建立起了对应的混沌数学模型和公式,如 Lorenz 混沌系统、Chen 混沌系统等等[5-6]. 通过对这些混沌系统运行轨迹的观测,数学家们发现,虽然已经建立了确定的数学模型,但混沌系统的轨迹仍然不是按照固定规律运行的,只是在概率意义上可以描绘出轨迹[7]. 此外,混沌系统对于初始状态也极为敏感,如果系统初值发生改变,其运行轨迹更加难以判断[8]. 近年来,在已经建立的三维混沌系统的基础上,数学家们又提出了超混沌数学理论,即在原有维度上进一步增加一维,变成四维混沌系统[9]. 相比于混沌系统,超混沌系统的复杂性、运行轨迹不可预测性更强,因此对于信息加密领域具有重要的应用价值[10].

从数学意义上看,混沌对于非线性动力学可以起到较好的诠释作用. 对于一般的运动形式而言,它都具有确定的运动规律和可以预测的运动轨迹. 但是,对于混沌运动而言,它虽然可以稳定在一个区域内运动,但其运动又是无规律可循的、运动轨迹又是不可以预测的. 所以,综合上述特征可以看出,混沌运动是典型的对立统一矛盾系统,运动规律上既有序又无序、运动轨迹上既确定又随机. 也正是因为混沌的这些特征,使其在非线性特征较强的领域都具有适用性.

本文在深入分析混沌数学理论、超混沌数学理论的基础上,将探讨其在图像加密领域中的应用效果.

1 超混沌理论

1.1 Lorenz 混沌系统

混沌数学理论的创立是由天体物理学和气象物理学所引发的. 其中,Lorenz 混沌系统是一个非常经典的混沌系统,它从大气的运动抽象而来,Lorenz 混沌系统在 3 个维度上可以用常微分方程描述,如公式(1)所示.

① 收稿日期:2017-01-09

作者简介:陈 敏(1982-),女,河南正阳人,硕士研究生,讲师,主要从事非线性泛函分析及应用数学研究.

$$\begin{cases}\dot{x} = -a(x-y)\\ \dot{y} = rx - y - xz\\ \dot{z} = xy - bz\end{cases} \tag{1}$$

这里，3个方程分别表示了 x,y,z 维度上的常微分方程；a,r,b 表示了整个 Lorenz 混沌系统的控制参数.

当3个控制参数按照 $a=16$，$r=45.92$，$b=4$ 确定取值时，如果 Lyapunov 指数 $\delta>0$，Lorenz 系统表现出混沌状态. 其混沌现象可以从不同的视角加以观察，如图1所示.

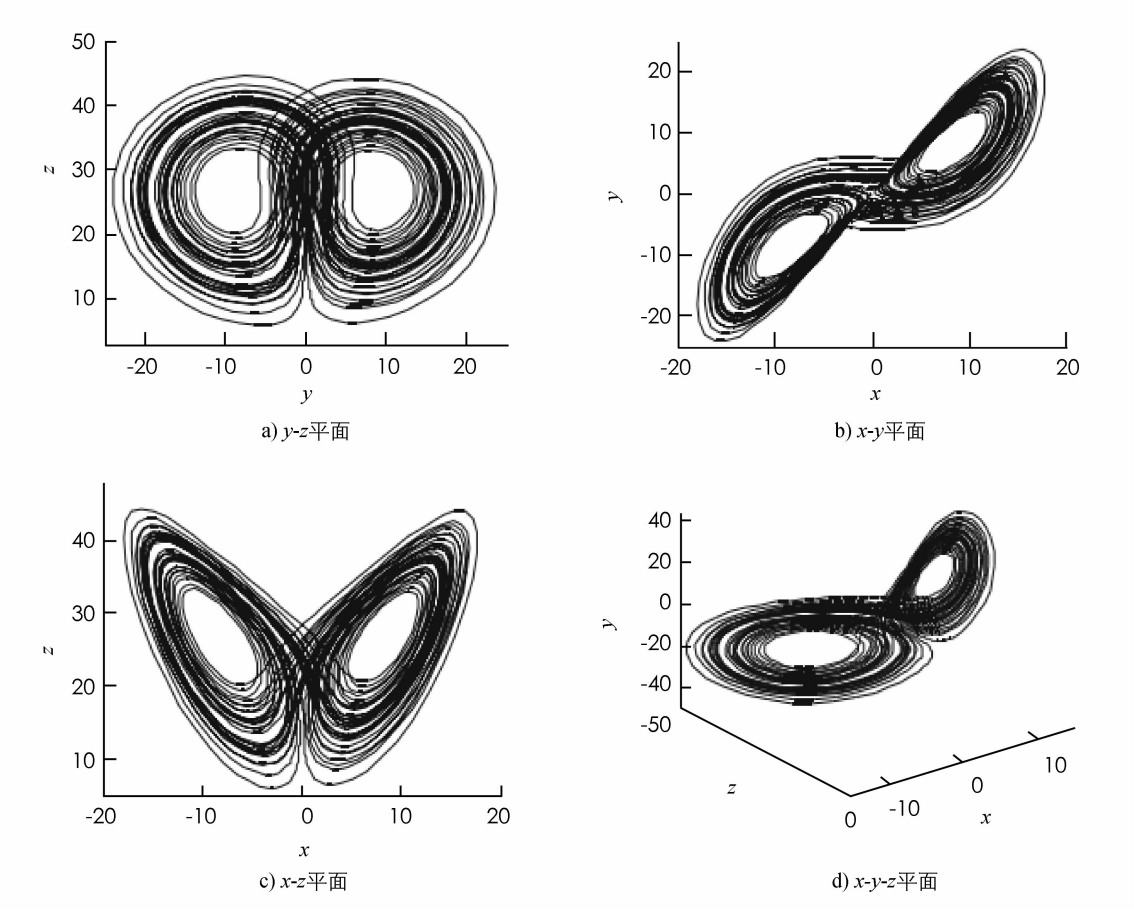


图1 Lorenz 系统的混沌状态

如图1所示，Lorenz混沌系统的轨迹围绕着2个白色的中心区域进行运转，2个白色中心区域就是整个混沌系统的吸引子.

1.2 Lorenz 超混沌系统

混沌系统因其鲜明的非线性动力学特征、运行轨迹的复杂多变、混沌状态对于初始值的敏感性，使其在很多领域中得到了应用.

为强化混沌系统的这些特征，有学者提出了超混沌数学理论. 所谓超混沌数学理论，就是在常规混沌系统的基础上，进一步增加混沌系统的维度，从而使其进一步满足 *Lyapunov* 指数判定原理，使其表现出更强的非线性动力学特征，运动轨迹更加随机变化，震荡过程进一步加剧.

按照这种思路，在 Lorenz 混沌系统的基础上，增加一个维度使其变成四维的超混沌系统，如公式(2)所示.

$$\begin{cases}\dot{x} = a(y-x)\\ \dot{y} = rx + cy - xz + w\\ \dot{z} = xy - bz\\ \dot{w} = -\mathrm{d}x\end{cases} \tag{2}$$

2　超混沌理论在图像加密中的应用

如前所述，混沌运动是典型的对立统一矛盾系统，本文将 Lorenz 超混沌系统运用于图像加密领域，通过实验效果来评价超混沌系统的优秀性能.

2.1　实验结果

在执行图像加密的过程中，将所有像素按照先上后下、从左到右、逐行排步的形式组合在一起，形成以像素为单位的数据序列，同时记录数据序列中的数据总数.

设$\{x(0), y(0), z(0), w(0)\}$是 Lorenz 超混沌系统一组状态的初始值，进而将这 4 个初始值分别代入公式(2)所示的超混沌系统，进而执行多次迭代处理，更新系统状态和位置，从而由初始状态生成一个新序列 $R=\{x(i), y(i), z(i), w(i)\}$，继而按照下面的方法，将不断出现的新序列合并为一个总序列 Q_k，如公式(3) 所示.

$$\begin{aligned}
&if(0\leqslant x_i<1) \qquad x_n=x_i; \qquad n=1,2,3,\cdots T/4\\
&if(-1\leqslant y_i<0) \qquad y_n=y_i; \qquad n=1,2,3,\cdots T/4\\
&if(0\leqslant z_i<1) \qquad z_n=z_i; \qquad n=1,2,3,\cdots T/4\\
&if(-1\leqslant w_i<0) \qquad w_n=w_i; \qquad n=1,2,3,\cdots T/4\\
&\quad for \qquad k=1:4:T\\
&\qquad\qquad Q_k=x_n;\\
&\qquad\qquad Q_{k+1}=y_n;\\
&\qquad\qquad Q_{k+2}=z_n;\\
&\qquad\qquad Q_{k+3}=w_n;\\
&\quad end
\end{aligned} \tag{3}$$

获得这个总的超混沌序列 Q 以后，对其进行等间隔划分形成 $M-1$ 个子区间，记录这些子区间的端点，根据这些端点再生成一个新序列 P_m，如公式(4) 所示.

$$p_m=Q_{1+(m-1)\cdot\frac{Q_T-Q_1}{M-1}} \tag{4}$$

这里，p_m 就表达了新序列 P_m 中的任意一个数据，也就是原始序列 Q 子区间的端点值. 再将这个新的数据序列 P_m 按照式(4) 执行计算处理，可以再次得到一个新的整数序列 O_m.

$$O_m=floor((abs(P_m*10\hat{}11)-foor(abs(P_m*10\hat{}11)))*10\hat{}3) \tag{5}$$

这里，*floor* 表示的是方向为负取整数，*abs* 表示的是取序列值的绝对值.

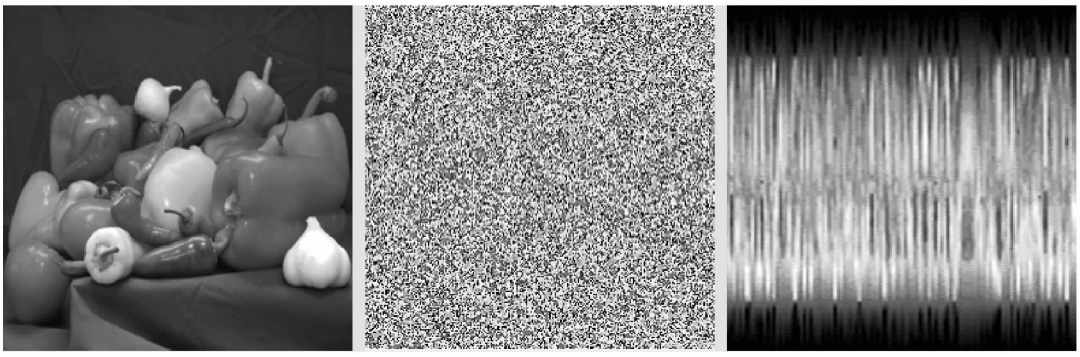
下面，就是要使得超混沌序列 O_m 和要加密的图像信息发生数学上的联系，具体的处理如公式(6) 所示.

$$N(m)=\mathrm{mod}(G*10000, O_m) \tag{6}$$

这里，超混沌序列 O_m 和要加密的图像信息被执行了取模的运算，G 则表达了原始图像数据序列中所对应的像素灰度信息，N 也可以看作是整个图像加密过程中的一个中间密钥结果.

按照上述思路构建基于 Lorenz 超混沌系统的图像加密方法，对彩色数字图像“辣椒”执行加密处理，其实验结果如图 2 所示.

如图 2(a)所示，“辣椒”的原始图像分辨率为 256 像素×256 像素，其画面中各种辣椒灰度差异大，背景区域明显. 执行了基于 Lorenz 超混沌系统的图像加密处理以后，加密结果如图 2(b)所示. 可以看出，“辣椒”加密图像中像素位置按照 Lorenz 超混沌运行轨迹置乱，置乱程度均匀，画面中已经无法观测到任何明文信息. 相比于本文方法的加密效果，使用三维 Loren 混沌完成的加密结果如图 2(b)所示. 可见，其加密效果的置乱程度均匀度明显低于本文方法.



(a) 原始图像 (b) 本文方法加密结果 (c) 三维混沌加密结果

图2 “辣椒”图像的加密效果

2.2 加密性能分析

为了进一步评价Lorenz超混沌系统在图像加密过程中的应用性能，本文采取3项相关性检测指标对加密实验的效果进行检测.

所谓三向相关性检测，就是指对一幅数字图像在水平方向上的相关性、垂直方向上的相关性、对角线方向上的相关性进行检测. 如果这3个方向上的相关性较高，证明这幅图像加密效果不好，更容易被攻击者破译；如果这3个方向上的相关性较低，证明这幅图像加密效果良好，不容易被攻击者破译. 三向相关性的计算，如公式(7)所示.

$$\begin{cases} E(x)=\dfrac{1}{N}\sum\limits_{i=1}^{N}x_i \\ D(x)=\dfrac{1}{N}\sum\limits_{i=1}^{N}(x_i-E(x))^2 \\ \operatorname{cov}(x,y)=\dfrac{1}{N}\sum\limits_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \\ r_{xy}=\dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\times\sqrt{D(y)}} \end{cases} \tag{7}$$

这里，r_{xy}用于表达相邻像素之间的相关程度，也称为相关系数；x与y用于表示执行相关性分析的2个像素的灰度或颜色信息.

按照公式(7)，对图2中“辣椒”的原始图像和加密结果分别执行三向相关性检测，结果如表1所示.

表1 “辣椒”图像的三向相关性检测结果

3个方向	“辣椒”原始图像	本文方法加密结果	三维Lorenz加密结果
水平方向相关性	0.862 5	0.001 2	0.217
垂直方向相关性	0.926 1	0.003 6	0.568
对角线方向相关性	0.951 8	0.002 9	0.097

从表1的结果可以看出，没有执行加密前，“辣椒”原始图像在3个方向上的相关性都接近1，相关程度非常高，安全性不高；经过基于Lorenz超混沌系统的图像加密处理之后，3个方向上的相关性都低于0.01，相关程度非常低，安全性高.

同时，可以看出一般的三维Lorenz混沌加密，加密后图像中水平和垂直方向上的相关性仍然很高，不够理想.

3 结 论

本文从混沌理论的基本概念谈起，阐述了混沌系统的判别方法，分析了Lorenz混沌系统的数学模型和吸引子状态图，并在Lorenz混沌系统的基础之上增加了一个维度，构建了Lorenz超混沌系统. 并基于Lorenz超混沌系统构建了一种图像加密方法，针对“辣椒”图像展开了图像加密实验研究. 实验结果表明，

基于 Lorenz 超混沌系统的图像加密方法可以获得理想的图像加密效果，加密结果中 3 个方向的相关性都比较低，这也间接表明了 Lorenz 超混沌系统的优秀性能.

参考文献：

[1] SABERY M K，YAGHOOBI M. A New Approach for Image Encryption Using Chaotic Logistic Map [C]. Phuket：International Conference on Advanced Computer Theory and Engineering，2008.

[2] 但建军，金渝光，高　瑾. 关于超空间复合系统混沌性的研究 [J]. 西南师范大学学报(自然科学版)，2016，41(10)：26－31.

[3] JOSHI M，SHAKER C，SINGH K. Image Encryption and Decryption Using Fractional Fourier Transform and Radial Hilbert Transform [J]. Optics and Lasers in Engineering，2008，46(7)：522－526.

[4] ZHU Z L，ZHANG W，WONG K K，et al. A Chaos-Based Symmetric Image Encryption Scheme Using a Bit-Level Permutation [J]. Information Sciences，2011，181(6)：1171－1186.

[5] 李丽香，彭海朋，杨义先，等. 基于混沌蚂蚁群算法的 Lorenz 混沌系统的参数估计 [J]. 物理学报，2007，56(1)：51－55.

[6] 张国山，牛　弘. 一个基于 Chen 系统的新混沌系统的分析与同步 [J]. 物理学报，2012，61(11)：137－147.

[7] LEONOV G A，KUZNETSOV N V，MOKAEV T N. Homoclinic Orbits，and Self-Excited and Hidden Attractors in a Lorenz-like System Describing Convective Fluid Motion [J]. The European Physical Journal Special Topics，2015，224(8)：1421－1458.

[8] 蔡　娜，井元伟，姜　囡，等. 超混沌 Chen 系统和超混沌 Lorenz 系统的反同步 [J]. 东北大学学报(自然科学版)，2009，30(3)：313－317.

[9] 唐　杰. 超混沌系统设计及其性能分析 [D]. 南京：南京航空航天大学，2007.

[10] 张　勇，尹社会，舒永录，等. 新超混沌系统模型的动力学分析 [J]. 华中师范大学学报(自然科学版)，2014，48(6)：806－811.

On Image Encryption Method Based on Hyper Chaos Theory

CHEN　Min，　GUAN Ying-zi

School of Mathematics and Statistics，Huanghuai University，Zhumadian Henan 463000，China

Abstract：The concept of chaos has been defined，and the method of chaos system been established based on Lypunov exponent. The mathematical model and attractor characteristics of Lorenz chaotic system have deeply been analyzed，and then the four-dimensional Lorenz chaotic system been constructed，which is called Lorenz hyperchaotic system. Compared with the Lorenz chaotic system，the Lorenz hyperchaotic system is more nonlinear and more random，so it is suitable for image encryption. The experimental results show that the image encryption method based on the Lorenz hyperchaotic system，the results of the encryption of the pixels in a row，three directional correlation.

Key words：Chaos Theory；Lorenz chaotic system；hyper chaotic system；image encryption

责任编辑　夏　娟