混沌加密算法与Hash函数构造研究

王　永
李昌兵　编著
何　波

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

混沌加密算法与 Hash 函数构造研究

王　永 李昌兵 何　波　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内容简介

本书紧跟混沌密码学的国际前沿，探讨了当前基于混沌理论的加密算法和 Hash 函数设计两项热点技术。在混沌基本理论和密码学的基础上，详细介绍了混沌分组密码、混沌流密码、混沌图像加密算法、混沌公钥密码和混沌 Hash 函数，以及混沌加密算法和 Hash 函数的安全性分析指标，探析了基于混沌的加密算法和 Hash 函数的最新国际研究成果，以及混沌密码算法设计的主要思路和发展趋势。

本书可作为高等院校数学、计算机、通信、信息安全等专业从事混沌密码研究的本科生、研究生、教师和科研人员的研究用书或参考资料。

图书在版编目（CIP）数据

混沌加密算法与 Hash 函数构造研究/王永，李昌兵，何波编著. —北京：电子工业出版社，2011.4

ISBN 978-7-121-13022-9

Ⅰ. ①混… Ⅱ. ①王… ②李… ③何… Ⅲ. ①计算机安全—加密技术 Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字（2011）第 033334 号

策划编辑：章海涛
责任编辑：李秦华
印　　刷：三河市鑫金马印装有限公司
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：720×1000　1/16　印张：13　　字数：291 千字
印　　次：2011 年 4 月第 1 次印刷
定　　价：32.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着计算机技术和网络技术的不断发展，计算机的应用范围日益广泛，管理信息系统、电子商务、电子政务、电子邮件以及网络游戏等应用已深入到了人们的日常工作和生活中，信息安全是其中不可缺少的部分，主宰着这些应用的进一步发展，是当前学术界和企业界共同关注的热点。加密算法和 Hash 函数是密码学中的两项基本技术，它们在保证信息安全的过程中发挥着重要的作用。

随着数字产品应用的不断深入和攻击手段的不断发展，迫切需要研究和开发出更多安全、高效、可靠的信息安全技术。将混沌理论引入信息安全领域是当前国际非线性科学和信息科学两个学科交叉融合的热门前沿课题之一，也得到了我国研究者的广泛重视。我国国家自然科学基金在 2003 年的重大研究项目“网络与信息安全研究计划”中就已将“复杂性理论在信息安全中的应用及密码算法分析研究”列入了计划，《国家中长期科学和技术发展纲要（2006—2020）》也在“核心数学及其在交叉领域的应用”这个重点领域内包括了“离散问题、随机问题、量子问题以及大量非线性问题中的数学理论和方法”等内容。

混沌和密码学之间具有天然的联系和结构上的某种相似性，启示着人们把混沌应用于密码学领域。比如传统的密码算法敏感性依赖于密钥，而混沌映射依赖于初始条件和映射中的参数；传统的加密算法通过加密轮次来进行扰乱和扩散，混沌映射则通过迭代，将初始域扩散到整个相空间。混沌系统是高度的非线性系统，具有伪随机性、遍历性和初值敏感性等特性，可以基于混沌设计出优秀的密码算法。此外，很多混沌系统与密码学常用的 Feistel 网络结构也非常相似。通过类比研究混沌理论与密码学，可以彼此借鉴各自的研究成果，促进共同发展。

2005 年初，我师从廖晓峰教授在重庆大学计算机学院攻读博士学位，研究方向为混沌密码算法的设计与分析，当时导师所领导的混沌密码学研究团队已经在国内外有了一定的知名度。在导师的指导下，我对混沌密码算法进行了比较深入的研究。博士毕业后，又到香港城市大学电子工程系参与了黄国和博士主持的快速混沌图像加密算法的研究。经过 5 年多的研究，我对混沌加密算法的设计和 Hash 函数的构造有了较为深刻的认识和见解。

当前，我国已有许多高等院校的学者、硕士生和博士生投入到了混沌密码学的研究过程中。回顾自己当初开始混沌密码研究之时，国内少有关于混沌密码的著作，国外也很难找到较为全面的论著，只能靠收集相关的学术论文，逐步了解混沌密码的相

关知识、发展历程、研究现状和最新的成果，真是一个漫长而艰苦的过程。为了让初次进入混沌密码方向的研究人员能够更便捷地了解这门学问，我萌发了编写本书的想法。在本书的安排上，首先从混沌和混沌密码的基本概念谈起，然后分加密算法的设计和 Hash 函数的构造，介绍当前具有代表性的典型算法，分析其设计思路、性能评价标准，并将自己的研究成果融入其中。一方面是帮助初涉混沌密码研究的学者能够更方便地掌握混沌密码的现状和最新研究动向，另一方面是为该领域的学者提供一些有价值的加密算法和 Hash 函数的设计方法，增进彼此之间的学术交流。

在编写本书时，我们对国内外大量的文献资料进行了精心的筛选和重新组织，并将自己的一部分研究成果和研究过程中的体会也撰写到了其中，全书分为三部分。

第一部分为混沌理论与密码学基础。主要介绍混沌的定义、运动特征以及混沌运动的判断准则，密码学基础知识和混沌密码学所涉及的主要研究内容。

第二部分为混沌加密算法的设计与分析。主要介绍基于混沌的对称加密算法、非对称加密算法和基于混沌的图像加密算法三个方面的内容，对其中具有代表性的算法进行了详细的介绍，并分析了它们的设计思路与安全性。在这部分还分析了针对混沌加密算法的主要攻击方法，并对混沌加密算法设计中应考虑的问题进行归纳与总结。

第三部分为基于混沌的 Hash 函数构造方法。主要从基于简单混沌系统和基于时空混沌系统两个方面讨论如何构造 Hash 函数，并对 Hash 函数的安全性评价进行了归纳和总结。

本书第 1 章和第 5 章由李昌兵编写，第 3 章由何波编写，其余章节由王永编写。全书由王永统稿和审定。杜茂康参与了本书编写大纲的制定，书稿编辑和校审等工作。

本书得到了国家自然科学基金项目“混沌系统数字化特性研究及其快速密码算法设计（61003256）”，重庆市自然科学基金项目“数字混沌技术在移动电子支付安全中的应用研究（CSTC，2009BB2282）”和“重庆邮电大学出版基金项目”等的资助，在此表示感谢！

感谢重庆大学廖晓峰教授多年对我所给予的指导、大量的支持和帮助，感谢香港城市大学电子工程系黄国和博士所给予的各种帮助！在本书的编写过程中，参考了很多国内外专家和同行学者的论文，在此诚向这些专家和学者表示衷心的感谢！

由于作者水平有限，书中不足之处在所难免，敬请读者批评指正。

目　录

第 1 章　混沌理论基础与混沌密码学的发展

混沌是一种貌似无规则的运动，指在确定性非线性系统中，不需要附加任何随机因素也可能出现类似的随机行为（内在随机性）[1]。混沌科学是随着现代科学技术的迅猛发展，尤其是在计算机技术的出现和普遍应用的基础上发展起来的新兴交叉学科。在物质世界中，混沌现象无处不在，大至宇宙，小至基本粒子，无不受混沌理论的支配。数学、物理、化学、生物、哲学、经济学、社会学、音乐、体育等领域中均存在混沌现象，它打破了不同学科之间的界线，是涉及系统总体本质的一门新兴学科。

在现代社会，最早研究混沌理论的学者是法国数学家庞加莱（H. Poincare），他于 1913 年在研究能否从数学上证明太阳系的稳定性问题时，把动力学系统和拓扑学有机地结合起来，并提出三体问题①在一定范围内的解是随机的，这实际上是一种保守系统中的混沌。1927 年，丹麦电气工程师 Van del Pol 在研究氖灯张弛振荡器的过程中，发现了一种重要的现象并将它解释为“不规则的噪声”，即所谓 Van del Pol 噪声。1954 年，前苏联概率论大师柯尔莫哥洛夫（Kolmogorov），在探索概率起源的过程中，提出了 KAM 定理的雏形，为早期明确不仅耗散系统有混沌现象而且保守系统也有混沌现象的理论铺平了道路。1963 年，美国麻省理工学院的气象学家洛伦兹（Lorenz）在研究大气环流模型的过程中，提出了“决定论非周期流”的观点，讨论了天气预报的困难和大气湍流现象，给出了著名的洛伦兹方程[2]。这是第一个在耗散系统中由一个确定的方程导出混沌解的实例，从此以后，关于混沌理论的研究正式揭开了序幕。

1.1　混沌理论基础

1.1.1　混沌的定义

混沌一词最早由李天岩(Li T Y)和约克(Yorke J A)于 1975 年提出。他们在“周期

① 所谓三体问题是指三维空间中的三个星体，在只有万有引力的作用下，给定它们的初始位置和速度，星体会怎样运动。三体问题的一个简单例子为太阳系中太阳，地球和月球的运动。

三意味着混沌”的文章中给出了混沌的一种数学定义[3]，现称为 Li-Yorke 定义：

区间 I 上的连续自映射 $f(x)$，如果满足下面条件：

① f 的周期点的周期无上界；

② 闭区间 I 上存在不可数子集 S，满足：

1） $\forall x, y \in S, x \neq y$ 时，$\limsup_{n\to\infty}\left|f^n(x)-f^n(y)\right|>0$；

2） $\forall x, y \in S$，$\liminf_{n\to\infty}\left|f^n(x)-f^n(y)\right|=0$；

3） $\forall x \in S$ 和 f 的任意周期点 y，有 $\limsup_{n\to\infty}\left|f^n(x)-f^n(y)\right|>0$；

则称 f 在 S 上是混沌的。

在此定义中，前两个极限说明子集的点 $x, y \in S$ 相当分散又相当集中；第三个极限说明子集不会趋近于任意周期点，所以此定义只预言了非周期轨道的存在，但不涉及这些非周期点的集合是否具有非零测度，也不涉及哪个周期是稳定的。所以 Li-Yorke 定义的缺陷在于集合 S 的勒贝格测度可能为零，即此时的混沌是不可观测的，而人们感兴趣的是可观测的情形，即 S 有一个正的测度。

根据 Li-Yorke 定义，美国学者 Richard H. Day 认为混沌系统应具有如下性质[1]：第一，存在所有阶的周期轨道；第二，存在一个不可数集合，该集合只含有混沌轨道，且任意两个轨道既不趋向远离也不趋向接近，而是两种状态交替出现，同时任一轨道不趋于任一周期轨道，即该集合不存在渐近周期轨道；第三，混沌轨道具有高度的不稳定性。

1989 年 Devaney R. L 给出了混沌的又一种定义[1]：

设 V 是一个度量空间，连续映射 $f: V \to V$，如果满足下面 3 个条件，则称 f 在 V 上是混沌的：

1）对初值的敏感依赖性：存在 $\delta>0$，对于任意的 $\varepsilon>0$ 和任意 $x \in V$，在 x 的 ε 邻域内存在 y 和自然数 n，使得 $d(f^n(x), f^n(y))>\delta$；

2）拓扑传递性：对于 V 上的任意一对开集 Z，$Y \in V$，存在 $k>0$，使 $f^k(Z) \bigcap Y \neq \Phi$；

3）f 的周期点集在 V 中稠密。

对于初值的敏感依赖性，意味着无论 x, y 离得多么近，在 f 的作用下，两者的轨道都可能分开较大的距离，而且在每个点 x 附近都可以找到离它很近而在 f 的作用下最终分道扬镳的点 y。对这样的 f，如果用计算机计算它的轨道，任何微小的初始误差，经过若干次迭代以后都将导致计算结果的失效。

拓扑传递性意味着任一点的邻域在 f 的作用之下将“撒遍”整个度量空间 V，这说明 f 不可能细分或不能分解为两个在 f 下不相互影响的子系统。

一般而言，上述两条是随机系统的特征，但第三条——周期点集的稠密性，却又

表明系统具有很强的确定性和规律性，绝非一片混乱，而是形似紊乱实则有序，这也正是混沌的耐人寻味之处。

除了上述对混沌的定义之外，还有诸如 Smale 马蹄、横截同宿点、拓扑混合以及符号动力系统等定义。然而，迄今为止，混沌一词还没有一个公认的普遍适用的数学定义[4, 5]。多数学者认为，给出混沌的精确定义是一件相当困难的事情，因为：不使用大量的技术术语不可能定义混沌；从事不同领域的人使用的混沌定义有所不同。突变论的创始人 Thom 更是认为“混沌”不可能有严格的数学定义。当前，尽管混沌尚无精确的定义，但从事不同领域研究的学者却已基于各自对混沌的理解进行了研究并谋求各自的应用。

1.1.2 混沌的运动特征

混沌运动是确定性非线性系统所特有的复杂运动形态，出现在某些耗散系统、不可积 Hamilton 保守系统和非线性离散映射系统中。混沌是一种不稳定的有限定常运动，它的定常状态不是通常概念下确定性运动的三种状态：静止（平衡）、周期运动和准周期运动，而是一种始终局限于有限区域且轨道永不重复的、形态复杂的运动。为了与其他复杂现象相区别，混沌运动有着自己独有的特征[6-9]：

① 有界性：混沌是有界的，它的运动轨道始终局限于一个确定的区域，这个区域称为混沌吸引域。无论混沌系统内部多么不稳定，它的轨道都不会走出混沌吸引域。所以从整体上说混沌系统是稳定的。

② 内随机性：在完全确定的系统内部产生的随机性被称为内随机性。混沌常被称为自发混沌、确定的随机性等，主要强调的就是混沌现象产生的根源在系统自身，而不是外部的影响。内随机性的另一方面是局部不稳定性。所谓稳定性是指系统受到微小扰动后保持原状态的属性或能力。所谓局部不稳定性是指系统运动的某些方面（如某些维度上）的行为强烈地依赖于初始条件。即初始条件的任何微小变化，经过混沌系统的不断放大，都有可能对其未来的状态造成极其巨大的差别。正是由于混沌轨道的不稳定性和对初始条件的敏感性，故不可能对混沌系统的长期行为进行预测。

③ 分维性质：混沌具有分维性质，但其非整数维不是用来描述系统的几何外形，而是用来描述系统运动轨道在相空间的行为特征。系统变化在相空间中可用一条轨道线来描述。混沌运动在相空间中某个区域内无限次的折叠，构成一个有无穷层次的自相似结构——奇怪吸引子。

④ 普适性：在混沌的转变中出现某种标度不变性，代替通常的空间或时间周期性。所谓普适性，是指不同系统在趋向混沌时所表现出来的共同特性，它不以具体的系数及系统的运动方程而变。普适性有两种，即结构的普适性和测度的普适性。前者是指趋向混沌的过程中轨线的分岔情况与定量特性不依赖于该过程的具体内容，而只

与它的数学结构有关；后者是指同一迭代在不同测度层次之间的嵌套结构相同，结构的形态只依赖于非线性函数展开的幂次。

⑤ 遍历性：混沌运动在其混沌吸引域内是各态历经的，即在有限时间内混沌轨道经过混沌区内每一个状态点。

1.1.3 混沌的判断准则

混沌来自于系统的非线性性质，但是非线性只是产生混沌的必要条件而非充分条件。那么，对于一个给定系统该如何判断它是否具有混沌特性？以及能否用数学语言说明混沌运动并对它进行定量刻画呢？这是混沌学研究的重要课题之一。下面将介绍几种常用的可作为混沌诊断与判据的方法[1, 6-11]。

① Lyapunov 指数

对于非线性动力学系统的完善定性描述，由于可能出现不规则运动而成为一个似乎是不可能解决的问题。如果附加应用统计方法，情况会好一些。目前在表征混沌运动方法方面，显示出重大意义的统计特征值之一是 Lyapunov 指数。它是相空间中相近轨道的平均收敛性或平均发散性的一种度量。

设 F 是 $R^n \to R^n$ 上的 n 维映射，它决定着一个 n 维离散动力系统：

$$x_{n+1} = F(x_n) \tag{1.1}$$

将系统的初始条件设为一个无穷小的 n 维的球，由于演变过程中的自然变形，球将变为椭球。将椭球的所有主轴按其长度顺序排列，那么第 i 个 Lyapunov 指数根据第 i 个主轴的长度 $P_i(n)$的增量加速率定义为：

$$\mathrm{LE}_i = \lim_{n\to\infty} \frac{1}{n} \ln\left[\frac{P_i(n)}{P_0(n)}\right] \tag{1.2}$$

Lyapunov 指数是与相空间的轨道收缩或扩张相关联的，在 Lyapunov 指数小于零的方向上轨道收缩，运动稳定，对初值不敏感；而在 Lyapunov 指数为正的方向上，轨道迅速分离，对初值敏感。通常将这 n 个 Lyapunov 指数按从大到小的顺序进行排列，将它们称之为 Lyapunov 指数谱：

$$\mathrm{LE}_1 \geqslant \mathrm{LE}_2 \geqslant \cdots \geqslant \mathrm{LE}_n$$

对于混沌，必定有一个 Lyapunov 指数是正的。因此，人们只要在计算中得知吸引子中有一个正的 Lyapunov 指数，即使不知道它的具体大小，也可以马上判定它是奇怪吸引子，而运动是混沌的。

由于工程中常通过计算最大 Lyapunov 指数来判断系统是否是混沌的，因此这里简要介绍一下一维混沌系统、差分方程组和微分方程组计算 Lyapunov 指数的方法。

1）一维混沌系统计算 Lyapunov 指数

考虑一维映射：$x_{n+1} = F(x_n)$，假设 x_n 有偏差 $\mathrm{d}x_n$，并导致 x_{n+1} 偏差 $\mathrm{d}x_{n+1}$，则：

$$x_{n+1}+\mathrm{d}x_{n+1}=F(x_n+\mathrm{d}x_n)\approx F(x_n)+\mathrm{d}x_n\cdot F'(x_n)\text{，即 }\mathrm{d}x_{n+1}=\mathrm{d}x_n\cdot F'(x_n)$$

设轨道按指数规律分离，即

$$|\mathrm{d}x_{n+1}|=|\mathrm{d}x_n|\cdot \mathrm{e}^{LE} \tag{1.3}$$

其中 LE 为 Lyapunov 指数。为了得到稳定的值，通常要取足够的迭代次数：

$$\mathrm{d}x_n=\mathrm{d}x_{n-1}\cdot F'(x_{n-1})=\mathrm{d}x_{n-2}\cdot F'(x_{n-2})\cdot F'(x_{n-1})=\cdots=\mathrm{d}x_0\prod_{i=0}^{n-1}F'(x_i)$$

因此

$$\mathrm{LE}=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\ln|F'(x_i)| \tag{1.4}$$

2）差分方程组计算 Lyapunov 指数

设 R^n 空间上的差分方程：$x_{i+1}=f(x_i)$，f 为 R^n 上的连续可微映射。f 的 Jacobi 矩阵为：

$$\boldsymbol{f}'(x)=\frac{\partial f}{\partial x}=\begin{bmatrix}\dfrac{\partial f_1}{\partial x_1},\cdots,\dfrac{\partial f_1}{\partial x_n}\\ \vdots\qquad\qquad\vdots\\ \dfrac{\partial f_n}{\partial x_1},\cdots,\dfrac{\partial f_n}{\partial x_n}\end{bmatrix}$$

令

$$J_i=f'(x_0)\cdot f'(x_1)\cdots f'(x_{i-1}) \tag{1.5}$$

将 J_i 的 n 个复特征根取模后，依从大到小的顺序排列为：

$$|\mathrm{LE}_1^{(i)}|\geqslant|\mathrm{LE}_2^{(i)}|\geqslant\cdots\geqslant\mathrm{LE}_n^{(i)}|$$

那么，f 的 Lyapunov 指数定义为

$$\mathrm{LE}_k=\lim_{i\to\infty}\frac{1}{i}\ln|\mathrm{LE}_k^{(i)}|,(k=1,\cdots,n) \tag{1.6}$$

该定义是计算差分方程组的最大 Lyapunov 指数 LE_1 的理论基础。

3）微分方程组计算最大的 Lyapunov 指数

设在由给定微分方程组所确定的相空间中，选取两条相轨迹起点差距为 d_0，经过时间 τ 后，呈指数分离，差距为 d_τ，即

$$d_\tau=d_0\mathrm{e}^{\tau\mathrm{LE}} \tag{1.7}$$

则 Lyapunov 指数为

$$\mathrm{LE}=\frac{1}{\tau}\ln\frac{d_\tau}{d_0} \tag{1.8}$$

数值计算时，从一条参考轨迹上找一个起点，算出相邻相轨的 d_0、d_τ，若 d_τ 不按指数增长，另找新起点计算 d_0、d_τ，为避免计算时出现发散，经过时间 τ 后，选取一个新起点，但与参考相轨迹的距离保持为 d_0。这样每次都是从距离为 d_0 的两个

状态出发，得到一系列 $d_1, d_2, \cdots, d_j, \cdots$ 最后按下式平均，得到最大 Lyapunov 指数：

$$\mathrm{LE}_1 = \lim_{n\to\infty} \frac{1}{n\tau} \sum_{i=1}^{n} \ln \frac{d_i}{d_0} \tag{1.9}$$

当 d_0 很小，而循环次数 n 极大时，只要 τ 不太大，计算结果就与 τ 的大小无关。利用计算机可以实现这种算法，得到一个可靠的 LE_1，进而可以判断系统运动是否为混沌的。

② Kolmogorov 熵

考虑一个 n 维动力系统，将它的相空间分割为多个边长为 ε 的 n 维立方体盒子，对于状态空间的一个吸引子和一条落在吸引域中的轨道 $x(t)$，取时间间隔为一个很小量 t，令 $P(i_0, i_2, \cdots i_d)$ 表示起始时刻系统轨道在第 i_0 格子中，$t=1$ 时在第 i_1 个格子中…，$t=d$ 时在第 i_d 个格子中的联合概率，则 Kolmogorov 熵定义为

$$K = -\lim_{t\to 0} \lim_{\varepsilon\to 0} \lim_{d\to 0} \frac{1}{\mathrm{d}t} \sum_{i_0 \cdots i_d} P(i_0, i_1, \cdots i_d) \ln P(i_0, i_1, \cdots, i_d) \tag{1.10}$$

由 K 熵的取值可以判断系统运动的无规则程度。对于确定性系统规则运动（包括不动点、极限环、环面），其 K 熵为 0；对于随机运动，其 K 熵趋于无穷；当 K 熵为一正数时则为混沌运动，且 K 熵值越大，混沌程度越严重。

③ 功率谱法

功率谱是一种表征复杂时间序列特征的统计量，是研究混沌的一种重要手段，也是计算机实验和实验室观测分岔和混沌的重要方法。下面简要介绍实际测量功率谱的计算方法。

在实际测量中得到的往往是按等时间间隔 t 的时间序列 $x_1, x_2, \cdots, x_N$。对此序列人为地加上周期边界条件 $x_{N+j} = x_j$，对任意的 j，计算其自相关函数，即离散卷积

$$c_j = \frac{1}{N} \sum_{i=1}^{N} x_i x_{i+j} \tag{1.11}$$

再对 c_j 做离散傅里叶变换，计算其傅里叶系数：

$$p_k = \sum_{i=1}^{N} c_j \mathrm{e}^{2\pi kj\sqrt{-1}/N} \tag{1.12}$$

p_k 表示第 k 个频率分量对 x_i 的贡献，即功率谱的本来意义。利用快速傅里叶变换，更有效的计算功率谱的方法是不经过自相关函数，直接求 x_i 的傅里叶系数，即

$$a_k = \frac{1}{N} \sum_{i=1}^{N} x_i \cos\left(\frac{\pi ik}{N}\right) \tag{1.13}$$

$$b_k = \frac{1}{N} \sum_{i=1}^{N} x_i \sin\left(\frac{\pi ik}{N}\right) \tag{1.14}$$

然后，计算 $p'_k = a_k^2 + b_k^2$，由许多组 $\{x_i\}$ 得到一批 $\{p'_k\}$，计算其平均值即可得到前面定义的功率谱 p_k。

对于周期运动，功率谱只在基频及其倍频处出现尖峰。准周期对应的功率谱在几个不可约的基频以及由它们叠加的频率处出现尖峰。混沌运动的功率谱为连续谱，会出现噪声背景和宽峰。

④ 庞加莱截面法

通过相空间的几何直观方法可表述动力学系统的各种形态。利用这种相图的方法可以把复杂运动简化。但是对于有些复杂运动，利用此方法进行研究是非常困难的，比如某些倍周期运动的倍数是很高的，其轨道看起来可能很乱，很难与非周期运动相区别，此时可用庞加莱截面方法进行研究。

在多维相空间 $(x_1, \mathrm{d}x_1/\mathrm{d}t, x_2, \mathrm{d}x_2/\mathrm{d}t, \cdots, x_n, \mathrm{d}x_n/\mathrm{d}t)$ 中适当选取一截面，在此截面上某一对共扼变量如 $x_1, \mathrm{d}x_1/\mathrm{d}t$ 取固定值，称此截面为庞加莱截面。运动轨迹与此截面的交点称为庞加莱点。设记录得到的庞加莱点依次为 $P_0, P_1, \cdots, P_n, \cdots$。原来相空间的连续轨迹在庞加莱截面上便表现为一些离散点之间的映射 $P_{n+1} = \mathrm{TP}_n$，由它们可得到关于运动特性的信息。只考虑庞加莱截面上的稳态图像，当庞加莱截面上只有一个不动点和少数离散点时，可判定运动是周期的；当庞加莱截面上是一封闭曲线时，可判定运动是准周期的；当庞加莱截面上是成片的密集点，且有层次结构时，可判定运动处于混沌状态。

⑤ 分维数分析法

分形理论是描述混沌信号的另一种手段。分形是没有特征长度但具有一定意义的自相似图形的总称。分形最主要的特性是自相似性，即局部与整体存在某种相似。

混沌的奇怪吸引子是轨道在相空间中经过无数次靠拢和分离，来回拉伸与折叠形成的几何图形，具有无穷层次的自相似结构。这种几何结构可用分维来描述，因此可以通过计算奇怪吸引子的空间维数来研究它的几何性质。

分维定义很多，常有以下几种形式：

1）盒维数：这是应用较广泛的维数概念之一。设 A 是 R^n 空间的任意非空有界子集，对每一 $\varepsilon > 0$，$N(A, \varepsilon)$表示用来覆盖 A 的半径为 ε 的最小封闭球数，如极限 $\lim\limits_{\varepsilon \to 0} \dfrac{\ln N(A,\varepsilon)}{\ln(1/\varepsilon)}$ 存在，则称：

$$D_k = \lim_{\varepsilon \to 0} \frac{\ln N(A,\varepsilon)}{\ln(1/\varepsilon)} \tag{1.15}$$

为盒维数。在实际计算中，可以构造一些边长为 ε 的盒子，然后计算不同 ε 值的盒子与 A 相交的个数 $N(A, \varepsilon)$，然后以 $-\ln \varepsilon$ 为横轴，$\ln N(A,\varepsilon)$为纵轴描出$[-\ln \varepsilon, \ln N(A,\varepsilon)]$，根据这些点组成的图形的斜率，便可以估计图形 A 的盒维数。

2）相似维数：由所有局部与整体相似的图形所组成的集合被称为自相似集。相似维数的定义为：

$$D_s(F)=-\frac{\ln m}{\ln(1/c)} \tag{1.16}$$

其中，m 是自相似集 F 中的相似子集的个数，c 为相似比例系数。

3）关联维数：关联维数是从实验数据中直接测定的一种维数，它较易计算，故应用很广，为描述复杂分形提供了一种新的手段。1983 年，Grassberger 和 Procaccia 提出了从时间序列中计算吸引子的关联维数的 G-P 算法。现简要介绍如下：

对于 n 维重构混沌动力系统，奇怪吸引子由点 $y_j=(x_j, x_{j+t}, x_{j+2t}, \cdots, x_{j+(n-1)t})$ 所构成。在构造好矢量 y_j 之后，需要先定义它们之间的距离。不妨将两个矢量的最大分量差作为距离，即 $|y_i-y_j|=\max\limits_{1\leqslant k\leqslant n}|y_{ik}-y_{jk}|$，并规定：凡是距离小于给定正数 r 的矢量，称为关联矢量。设重构相空间中有 N 个点(即矢量)，计算其中有关联的矢量对个数，它在一切可能的 N^2 种配对中所占的比例称为关联积分

$$C_n(r)=\frac{1}{N^2}\sum_{i,j=1}^{N}\theta(r-|y_i-y_j|) \tag{1.17}$$

式中 θ 为 Heaviside 单位函数：

$$\theta(x)=\begin{cases}0, & x\leqslant 0\\ 1, & x>0\end{cases} \tag{1.18}$$

关联积分 $C_n(r)$ 在 $r\to 0$ 时与 r 存在以下关系：

$$\lim_{r\to 0}C_n(r)\propto r^D \tag{1.19}$$

式中 D 称为关联维数，恰当选取 r，使得 D 能够描述混沌吸引子的自相似结构。由于式(2.19)有近似数值，故可得关联维数的计算关系

$$D=\frac{\ln C_n(r)}{\ln r} \tag{1.20}$$

4）Lyapunov 维数：从几何直观考虑，正 Lyapunov 指数代表的方向对吸引子起支撑作用，而负 Lyapunov 指数对应的收缩方向，在抵消膨胀方向的作用后，提供吸引子维数的非整数部分。因此，将 Lyapunov 指数从最大的 LE_1 开始，把后继的 Lyapunov 指数一个个加起来。若加到 LE_K 时，和 $\sum\limits_{i=1}^{k}LE_i$ 为正数，而加到下一个 LE_{K+1} 后，和 $\sum\limits_{i=1}^{k+1}LE_i$ 变成负数，则可以用线性插值来确定维数的非整数部分。吸引子的 Lyapunov 维数定义为：

$$d_L=K+\frac{1}{LE_{K+1}}\sum_{i=1}^{k}LE_i \tag{1.21}$$

式中 k 为使 $\sum\limits_{i=1}^{k}LE_i>0$ 成立的最大整数。

Lyapunov 维数对描述混沌吸引子非常有用，对 n 维相空间来说有以下结论：

定常吸引子：$LE_1<0, LE_2<0, \cdots, LE_n<0$，此时 Lyapunov 维数为 0，对应于平衡