

文章编号:1006-7329(2002)02-0092-05

分形图像的压缩编码和混沌保密通讯

杨帆

(武汉化工学院, 武汉 430073)

摘要:根据分形原理,利用邻域匹配二叉树算法,及棒-棒控制法实现了混沌在保密通信领域的稳定控制,按驱动-响应法设计了模拟电路,并用计算机模拟其同步。

关键词:分形; 二叉树算法; 保密通讯; 计算机模拟

中图分类号:TP391.4

文献标识码:A

在 ISDN、多媒体技术、HDTV 及信息高速公路飞速发展的今天,图像的存储和传输一直是关键技术之一。一幅图像的各像素之间存在着很大的相关性,利用编码的方法删去相关性,减少冗余,这就是图像压缩。图像压缩较为成熟的方法有变换编码、预测编码、矢量编码等,但这些方法压缩比有限,做得好可达 8~20 倍^[1]。由曼德布罗特(Mandelbrot)提出的分形几何学,以新的观念、新的手段处理大自然中非线性系统的复杂现象,利用图像的分形特性可以实现图像的大比例压缩,例如,枫叶图像的压缩比可达 1 365^[2]倍。由此可见,分形在图像压缩编码中有着广泛的应用前景,图像或文件在传输过程中,会遇到各种各样的问题,人们最关心的是通信的安全与快捷。而已有的保密方式经过长期的研究与解密,保密水平越来越低。人们总是从最新理论中找出适合于保密通讯方式,造成破译时的极度困难。混沌理论正是这样一门新型学科,由耗散系统产生,可以由确定的方式描述,对初始条件极为敏感,具有内禀随机性和长期预测不可能性。在应用中,把复杂的混沌信号混合在有用信号中,然后发射出去。由于混沌信号具有无限多个不稳定周期轨道,对初始条件极为敏感,故不易破译。混沌同步将成为保密通信的重要手段之一。本文利用分形理论进行图像压缩编码以及利用混沌进行保密通讯,有着重要的理论意义与实用价值。

1 分形图像的压缩编码和混沌保密通讯流程框图

本文主要讲述了对分形图像用邻域二叉树压缩编码算法,及混沌控制与混沌同步保密通信的设计与仿真,其具体流程框图如图 1。

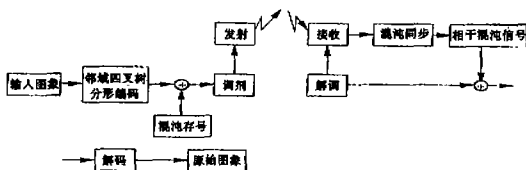


图 1 分形图像的压缩编码和混沌保密通讯流程框图

• 收稿日期:2001-11-28

作者簡介:杨帆(1966-),女,湖北公安,硕士,讲师,主要研究智能化仪器仪表、可编程控制器及计算机模拟研究。

2 分形、混沌及 IFS 迭代函数系统的基本原理

自然界的很多物体是不规则的,不是完美的直线或光滑的曲线,纯数学曲线只是实现物体的有用近似,而不能为某个物体提供完整的模型。分形正是解决这一难题的有效方法,具有如下特征的集合称为分形集:具有精细的结构;具有某种自相似的结构;分形维数大于它的拓扑维数;可以由迭代等方法产生。

现实世界的绝大部分不是有序、稳定和平衡的,而是无序、变化和涨落起伏的。混沌现象把表现的无序性与内在的规律性巧妙融为一体,通过分形论由表面现象去寻找内部的运动规律。混沌特征为^[2]:随机性;分维性;普适性;标度律。

所谓 IFS 就是一组压缩映射,本文中讨论的是它的逆问题:取给定的集 L ,对它作压缩变换,然后把它们粘贴在一起以便重构 L 。

3 邻域匹配四叉树压缩编码算法

邻域匹配四叉树压缩编码算法的基本思想是:从相对较大的区域开始,如 64×64 区域,并寻找最相似的较大区域。预先设定一门槛值,如果两个区域之间的误差值在门槛值之内,则把该区域标记为已处理过并把它加到区域映射表中去。如果超过了门槛值(没有合适的相似区域),则分解该子块并在更小的区域上重复该过程。

根据邻域匹配四叉树压缩编码算法的基本思路,给出程序框图如图 2。

4 混沌棒—棒控制原理及仿真电路图

4.1 混沌棒—棒控制原理

由于混沌吸引子对初始条件的敏感性和轨迹不重复性,使混沌控制十分困难。本文采用了洛仑兹

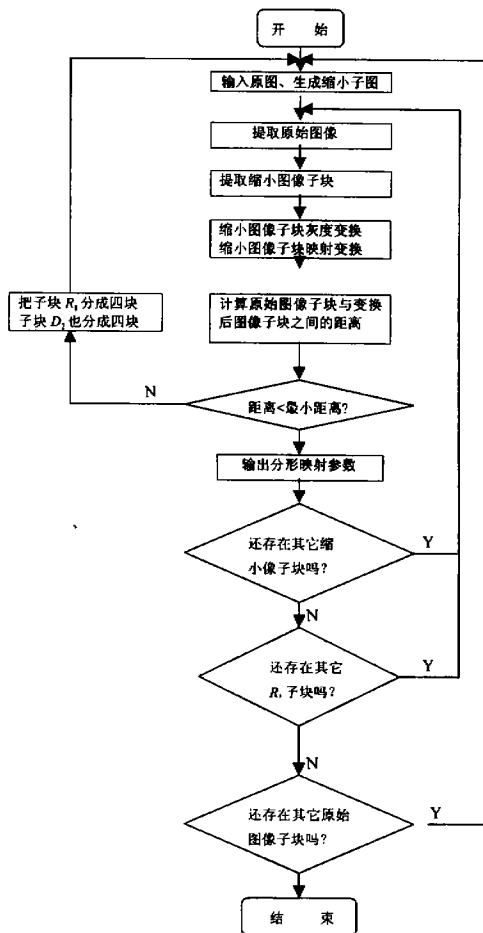


图 2 邻域匹配四叉树压缩编码算法程序框图

系统的棒—棒控制,即对洛伦兹方程右边加一个控制输入 u ,于是得到一个受控的 Lorenz 系统如下:

$$\begin{cases} \dot{x} = \sigma_x + \sigma_y \\ \dot{y} = rx - y - xz + u \\ \dot{z} = xy - bz \end{cases} \quad (1)$$

对受控的 Lorenz 系统,利用可控性最小值原理去确定一个控制以驾驭系统到达目标 C ,将 Lorenz 系数代入方程得 Bang-Bang 控制的开关曲面如下:

$$x^2 - \frac{8}{3}z = 0 \quad (2)$$

利用这个曲面写出欲施加的 Bang-Bang 控制如下:

$$u = -k \operatorname{sgn}(x^2 - \frac{8}{3}z) \quad (3)$$

当 $k=10$ 时 Lorenz 系统(1)在式(3)作用下的运动过程如下:

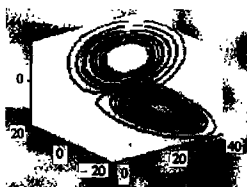


图3 任意的洛伦兹系统



图4 Bang-Bang 控制下的洛伦兹系统

由图可见,在 Bang-Bang 控制下的洛伦兹系统先环绕错误平衡点运动两周,然后进入正确平衡点的轨道,并沿着一条螺旋轨道渐进稳定到 $C(8.4853, 8.4853, 27)$ 。

在达到被指定的平衡点 C 后,根据 Lyapunov 指数的计算公式:

$$\lambda_1 = \lim_{t \rightarrow \infty} \frac{1}{t} \ln \frac{|\delta x_1(x_0, t)|}{|\delta(x_0, t)|} \quad (4)$$

所求得的 Lyapunov 指数为谱为 $(-0.6475, -0.4642, -0.5390)$,即对整个系统的 Lyapunov 指数均为负值,从而对系统实现了稳定控制。

由此可见,在 Bang-Bang 式(3)的作用下,不论从状态空间任何一点起始点时,系统将会改变稳定点 C ,它说明系统虽然终止在某一平衡点,但最终平衡状态出发,系统轨迹最终都能稳定到 $C=(8.4852, 8.4852, 27)$,只是在某些初始条件下,稳定时间较长。

4.2 洛伦兹系统的仿真电路图

在混沌掩盖中,类似噪声的混沌掩盖信号 $u(t)$ 加到信息信号 $m(t)$ 上,合成发送信号 $s(t) = u$

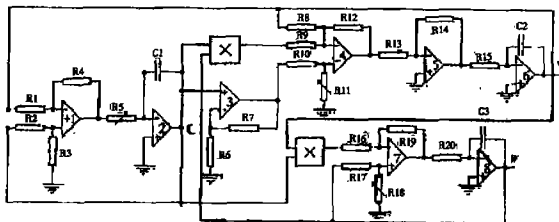


图5 洛伦兹系统的仿真电路图

$(t) + m(t)$ 发送出去。接受端的混沌电路在接收到的 $s(t)$ 的驱动下,两个混沌吸引子的轨迹彼此相互跟随,接收机中再生成掩盖信号 $u_c(t)$ 。从接收到的信号中抽去它,恢复出信息信号。基于上述原理设计的洛仑兹系统的仿真电路图如图 5。

5 误差分析

本文中利用洛仑兹系统作为牵引系统,构造两个子系统 (a) , (b) :

$$(a) \begin{cases} \dot{x}_1 = \sigma(y - x_1) \\ \dot{y}_2 = rx - y_2 - x_2 \end{cases}$$

$$(b) \begin{cases} \dot{x}_1 = x_1 y - bx_1 \\ \dot{z}_2 = x_2 y - bz_2 \end{cases}$$

其中,我们用驱动系统的 y 控制子系统 (a) ,用驱动系统的 x 控制子系统 (b) ,本文用 C++ 程序对所设计的洛仑兹系统同步误差进行分析。程序框图如图 6。

上述三个子系统的初始值完全不同,通过同步控制,最终同步。见图 7。用上述程序仿真的洛仑兹系统同步误差如图 8,当迭代 30 000 次以后,误差为 0.003 08,初始误差为 3,即相对误差为 1%。当迭代次数增加时,误差最终趋于零。

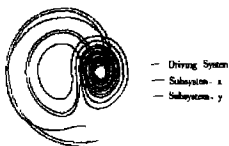


图 7 洛仑兹系统同步

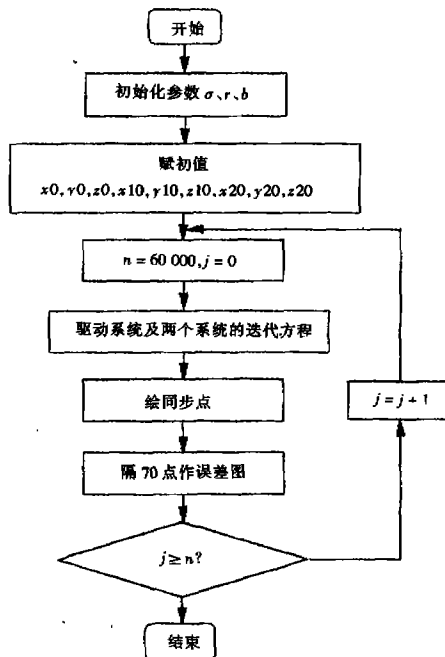


图 6 洛仑兹系统同步误差

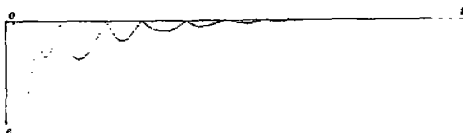


图 8 洛仑兹系统同步误差

6 结论

本文研究分形图像的压缩编码与混沌保密通信,讨论了图像存储与传输这两个基本问题。图像存储利用邻域四叉树算法,该算法提高了恢复图像质量和压缩比。图像传输利用了洛仑兹吸引子为混沌载体,用 bang-bang 控制法对它实现了鲁定控制,从模拟结果看,洛仑兹系统将鲁定于它的不动点上,接着用鲁定响应法设计了混沌同步电路;最后,模拟出驱动系统和响应系统之间的同步。从模拟结果看,系统的同步性很好。

参考文献:

- [1] 陈守洁, 张立明. 分形与图像压缩[M]. 上海科技教育出版社, 1998.
- [2] 皮明红, 彭高雄. 邻域匹配和分类匹配的分形块编码[J]. 中国图像图形学报, 1997, (5): 2.
- [3] 毕勤胜, 陈予恕. 混沌同步效应及在保密通信和现代管理中的应用[J]. 振动与冲击, 1999, (1): 18.
- [4] B. B. Mandelbrot. Let object fractals; forme, hazard et dimension[M]. Flammarion, 1975, 60—200.
- [5] Murali K, Lakshmanan M. Drive-response of Chaos synchronization in identical nonlinear system[J]. Physical Review E, 1994, (6): 49.

Compressed Code of Fractal Image and Secure Communication with Chaos

YANG Fan

(Wuhan Institute of Chemical Technology, Wuhan 430073, China)

Abstract: Based on the fractal theory, using quarter tree in neighborhood method and Bang—Bang control method, the steady control of the chaotic in the secure communication is realized. A simulation circuit has been designed based on driving responding theory, then, its synchronization is simulated on the computer.

Keywords: fractal; secure communication; computer simulation

(上接第 81 页)

Research on Indirect Financing Countermeasure for China's Medium and Small Sized Enterprises

CHEN Guo, WU De-fu

(Faculty of Construction Management and Real Estate, Chongqing University, Chongqing 400045, China)

Abstract: At present, it is difficult for medium and small enterprises in China to circulate funds. It is a key problem concerning China's economic development. Since the capital market of China still has a long way to go, it is realistic to discuss the indirect finance. This paper studies the indirect finance channels on two levels.

Keywords: medium and small enterprise; indirect finance; countermeasure