

# 基于多涡卷系统的多进制数字混沌键控方式

禹思敏<sup>1)</sup> 林清华<sup>2)</sup> 丘水生<sup>3)</sup>

<sup>1)</sup>(广东工业大学自动化学院, 广州 510090)

<sup>2)</sup>(广东工业大学应用物理系, 广州 510090)

<sup>3)</sup>(华南理工大学电子与信息学院, 广州 510640)

**摘要** 多涡卷混沌吸引子的主要特点是具有复杂的混沌动力学行为和多个螺旋密钥参数,可在保密通信中获得应用。在研究其产生机理的基础上,进一步提出了用多涡卷混沌系统实现多进制数字混沌键控(MDCSK)的一种方案。其工作原理是,在发送端,用多进制数字信号对多涡卷混沌吸引子的多个斜率值进行数字调制,从而产生多进制混沌键控信号。在接收端,根据驱动-响应式同步和相关解调原理恢复出原来的多进制数字信号。与二进制混沌键控(CSK)相比,多进制数字混沌键控(MDCSK)方式能体现出利用多个螺旋密钥参数来加密多进制数字信号这一主要优点。通过该方案的理论分析和计算机模拟结果,证实了这一方法的有效性。

**关键词** 多涡卷混沌吸引子 多进制数字混沌键控 驱动-响应式同步 相关解调

**中图分类号:** TN901 **文献标识码:** A **文章编号:** 1006-8961(2004)12-1473-07

## Multi-level Digital Chaos Shift Keying Based on Multi-scroll Chaotic Systems

YU Si-min<sup>1)</sup>, LIN Qing-hua<sup>2)</sup>, QIU Shui-sheng<sup>3)</sup>

<sup>1)</sup>(College of Automation, Guangdong University of Technology, Guangzhou 510090)

<sup>2)</sup>(Department of Applied Physics, Guangdong University of Technology, Guangzhou 510090)

<sup>3)</sup>(College of Electronic & Information Engineering, South China University of Technology, Guangzhou 510640)

**Abstract** The main feature of multiple-scroll chaotic attractors is that they exhibit a rich variety of complicated chaotic dynamic phenomena and have many scroll encryption parameters that can be applied to secure communications. Based on the study of their generating mechanism, a novel scheme of multi-level digital chaos shift keying (MDCSK) via multi-scroll chaotic systems is presented. In the transmitter, the slope values of the multiple scroll chaotic attractors are modulated using multi-level digital signals, which generates MDCSK signals. In the receiver, the original multi-level digital signals are recovered according to the principle of drive-response synchronization and coherent demodulation. Compared with chaos shift keying (CSK), MDCSK has an advantage that multi-level digital signals can be encrypted, by using multi-scroll encryption parameters. Results of theoretical analysis and computer simulation are also given, which demonstrates the effectiveness of the proposed method.

**Keywords** multiple scroll chaotic attractors, multi-level digital chaos shift keying (MDCSK), drive-response synchronization, coherent demodulation

## 1 引言

混沌信号以其宽带谱、冲击式的相关统计特性、对初始条件的高度敏感性、非周期性、似噪声且确定可再生等特点,在通信技术中有较为广泛的应用前

景。混沌通信主要有混沌模拟通信和混沌数字通信两大类,而后者将成为主要的通信方式<sup>[1,2]</sup>,其主要应用基于以下两个方面:(1)利用混沌信号的宽带谱特性,以混沌信号代替传统数字通信的周期基带信号,其主要代表为混沌键控(CSK)方式<sup>[3]</sup>,在此基础上发展成为 COOK、DCSK、FM-DCSK 等调制方式<sup>[4,5]</sup>;(2)利

用混沌序列的相关性能良好、码族数量众多和非周期的特点,可用混沌序列替代原来扩频通信中的伪随机序列而成为混沌数字扩频通信方式<sup>[6]</sup>。

在混沌通信系统中,如何产生适合于调制与扩频的混沌信号已成为人们所关注的问题,并提出了若干种用于产生混沌信号的方法<sup>[7~13]</sup>,其中有关多涡卷混沌吸引子的研究是近年来所取得的一个重要成果,产生多涡卷混沌吸引子的方法主要有多个分段线性法<sup>[10~12]</sup>和正弦函数法<sup>[13]</sup>,可通过硬件实验和计算机模拟产生多达 11~21 个以上涡卷的混沌吸引子<sup>[12]</sup>。多涡卷混沌吸引子的主要特点是具有更复杂的混沌动力学行为和更多的密钥参数,如多个不同的斜率和多个不同转折点值等。因此,可在混沌通信中获得应用。

在前期工作的基础上<sup>[12]</sup>,提出了一种用多涡卷混沌吸引子实现多进制数字混沌键控(MDCSK)的方案,其主要特点是利用  $N$  涡卷混沌吸引子所具有的  $N$  个不同斜率值  $M_i (i=0, 1, 2, \dots, N-1)$ , 实现  $M (M \leq N)$  进制数字混沌键控。以传送 4 进制数字信号为例,通过对 7 涡卷混沌吸引子中的各个涡卷的大小进行混沌数字键控,将每个数字符号  $\{b_i (i=1, 2, 3, 4)\}$  映射到 7 涡卷混沌吸引子的各个不同的涡卷之中,在发送端产生一个混沌扩频信号  $x^{(0)}(t)$ 。在接收端,根据驱动-响应式同步和相关解调原理,恢复出原来的 4 进制数字序列。该方法是文献<sup>[3]</sup>利用双涡卷混沌吸引子实现二进制数字混沌键控(CSK)的一种推广和扩充。

## 2 多涡卷混沌吸引子的产生与同步

1983 年,美国著名电学专家蔡少棠教授提出了蔡氏电路<sup>[7~9]</sup>,它是人类首次通过电子线路实验研

究和观察非线性电路与系统中混沌现象的先驱。蔡氏电路的主要特点是,利用三分段线性函数产生双涡卷,它由两个涡卷运动和一个键带运动产生,如图 1 所示。在蔡氏电路的基础上,文献<sup>[10]~[12]</sup>则提出了基于  $2N-1$  个分段线性函数产生  $N$  涡卷混沌吸引子,它由  $N$  个涡卷运动和  $N-1$  个键带运动产生,并研究了它的同步问题,为多涡卷吸引子用于混沌通信提供了前期研究。

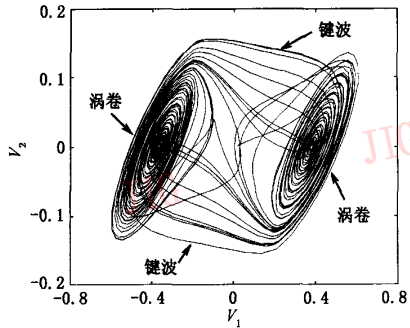


图 1 双涡卷混沌吸引子

根据文献<sup>[12]</sup>的研究结果,以  $N$  涡卷混沌吸引子为例,其无量纲归一化状态方程可表为

$$\begin{cases} dx^{(0)}/d\tau = \alpha[y^{(0)} - f(x^{(0)})] \\ dy^{(0)}/d\tau = x^{(0)} - y^{(0)} + z^{(0)} \\ dz^{(0)}/d\tau = -\beta y^{(0)} \end{cases} \quad (1)$$

根据驱动-响应式同步原理<sup>[14]</sup>,将驱动系统式(1)的状态变量  $x^{(0)}$  作为下式响应系统的驱动变量,则响应系统的状态方程可表为

$$\begin{cases} dx^{(1)}/d\tau = \alpha[y^{(1)} - f(x^{(1)})] \\ dy^{(1)}/d\tau = x^{(0)} - y^{(1)} + z^{(1)} \\ dz^{(1)}/d\tau = -\beta y^{(1)} \end{cases} \quad (2)$$

式中,  $\alpha=12, \beta=17.6$ 。其中  $f(x^{(k)}) (k=0, 1)$  为在两个系统中产生  $N (N=3, 4, 5, 6, 7, \dots)$  涡卷的  $2N-1$  个分段线性奇函数

$$f(x^{(k)}) = M_{N-1}^{(k)} x^{(k)} + 0.5 \sum_{i=1}^{N-1} (M_{i-1}^{(k)} - M_i^{(k)}) \cdot (|x^{(k)} + X_i^{(k)}| - |x^{(k)} - X_i^{(k)}|) \quad (3)$$

$$= \begin{cases} M_0^{(k)} x^{(k)} & (|x^{(k)}| < X_1^{(k)}) \\ M_i^{(k)} x^{(k)} + \sum_{j=1}^i (M_{j-1}^{(k)} - M_j^{(k)}) X_j^{(k)} \cdot \frac{|x^{(k)}|}{x^{(k)}} & (X_i^{(k)} \leq |x^{(k)}| < X_{i+1}^{(k)}, i = 1, 2, \dots, N-2) \\ M_{N-1}^{(k)} x^{(k)} + \sum_{j=1}^{N-1} (M_{j-1}^{(k)} - M_j^{(k)}) X_j^{(k)} \cdot \frac{|x^{(k)}|}{x^{(k)}} & (|x^{(k)}| \geq X_{N-1}^{(k)}) \end{cases}$$

式中,  $k=0$  代表驱动系统式(1)的参数,  $f(x^{(0)})$  为驱动系统式(1)的  $2N-1$  个分段线性函数;  $k=1$  代表响应系统式(2)的参数,  $f(x^{(1)})$  为驱动系统式(2)的  $2N-1$  个分段线性函数。  $M_i^{(k)} (i=0, 1, 2, \dots, N-1)$

为  $f(x^{(k)})$  中各个线性区间的斜率,  $X_i^{(k)} (i=1, 2, 3, \dots, N-1)$  为  $f(x^{(k)})$  的各个转折点值,任给一个初值  $X_1^{(k)}$ , 可用以下的递推公式来确定其余转折点  $X_i^{(k)} (i=2, 3, \dots, N-1)$ <sup>[12]</sup>

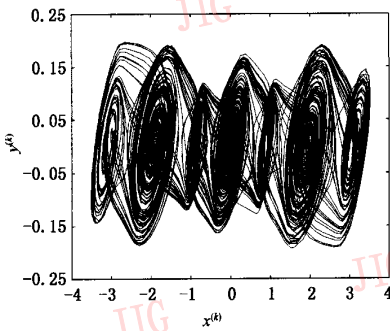
$$\left\{ \begin{aligned} X_2^{(k)} &= \frac{2 \sum_{i=1}^1 (M_i^{(k)} - M_{i-1}^{(k)}) X_i^{(k)}}{M_1^{(k)}} - X_1^{(k)} \\ X_3^{(k)} &= \frac{2 \sum_{i=1}^2 (M_i^{(k)} - M_{i-1}^{(k)}) X_i^{(k)}}{M_2^{(k)}} - X_2^{(k)} \\ &\dots\dots \\ X_{N-2}^{(k)} &= \frac{2 \sum_{i=1}^{N-3} (M_i^{(k)} - M_{i-1}^{(k)}) X_i^{(k)}}{M_{N-3}^{(k)}} - X_{N-3}^{(k)} \\ X_{N-1}^{(k)} &= \frac{2 \sum_{i=1}^{N-2} (M_i^{(k)} - M_{i-1}^{(k)}) X_i^{(k)}}{M_{N-2}^{(k)}} - X_{N-2}^{(k)} \end{aligned} \right. \quad (4)$$

现以 7 涡卷 ( $N=7$ ) 混沌吸引子为例, 根据式(4), 可确定  $f(x^{(k)})$ , 其中的一组参数为

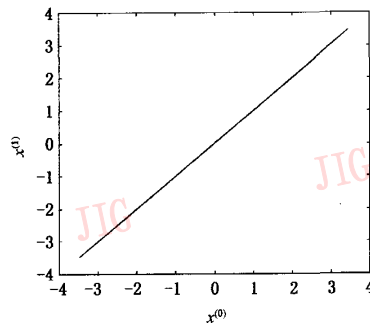
$$\left\{ \begin{aligned} [M_0^{(k)}, M_1^{(k)}, M_2^{(k)}, M_3^{(k)}, M_4^{(k)}, M_5^{(k)}, M_6^{(k)}] &= \\ [0.170, -0.432, 0.380, -0.426, 0.127, -0.406, 0.227] \\ [X_1^{(k)}, X_2^{(k)}, X_3^{(k)}, X_4^{(k)}, X_5^{(k)}, X_6^{(k)}] &= \\ [0.4000, 0.7148, 1.0727, 1.3920, 2.4628, 2.7978] \end{aligned} \right. \quad (5)$$

设驱动系统式(1)与响应系统式(2)的参数相同, 如上所述, 根据式(1)~(5), 可得驱动系统与响应系统的 7 涡卷混沌吸引子及其同步相图的计算机模拟结果如图 2 所示。

另一方面, 若驱动系统(1)与响应系统(2)的参数不匹配, 则不能实现同步。例如, 在参数  $M_0^{(0)}$  与  $M_0^{(1)}$  不匹配的情况下, 设  $M_0^{(0)} = 0.170$ ,  $M_0^{(1)} = M_0^{(0)} + \Delta M_0^{(0)}$ ,  $\Delta M_0^{(0)} = 0.01$ , 驱动系统与响应系统处于失步状态, 计算机模拟结果如图 3 所示。可利用上述原理实现多进制数字混沌键控。

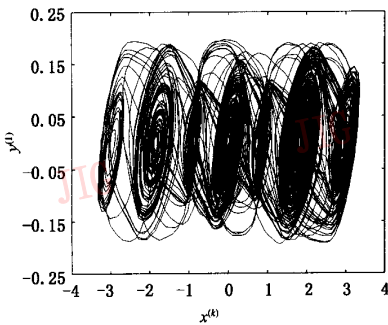


(a) 驱动系统与响应系统同步时 7 涡卷混沌吸引子 ( $k=0.1$ )

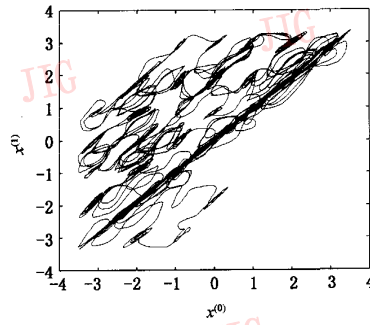


(b) 驱动系统与响应系统的同步相图

图 2 驱动-响应式同步时的 7 涡卷混沌吸引子及同步相图



(a) 失步时响应系统的 7 涡卷混沌吸引子



(b) 驱动系统与响应系统的失步相图

图 3 参数不匹配 ( $M_0^{(0)} \neq M_0^{(1)}$ ) 时的 7 涡卷混沌吸引子及失步相图

### 3 MDCSK 方案

一种基于多涡卷混沌吸引子的 MDCSK 如图 4

所示。在发送端, 设有 4 进制数字序列  $\{\dots b_1, b_3, b_2, b_4, b_3, b_1, b_4, b_2, \dots\}$  对发送端的 7 涡卷混沌吸引子中分段线性函数  $f(x^{(0)})$  的 4 个斜率值  $[M_0^{(0)}, M_2^{(0)}, M_4^{(0)}, M_6^{(0)}]$  实现混沌键控, 即对发送端 7 涡卷混沌吸引子中各个涡卷的大小进行数字调制。例如, 当输

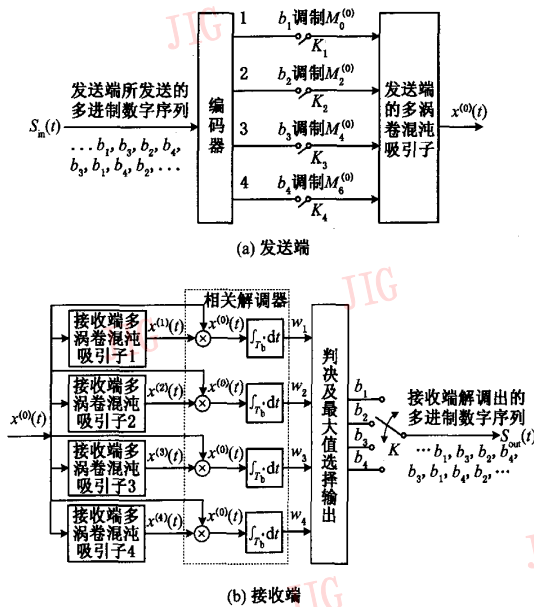


图4 基于多涡卷混沌吸引子的MDCSK系统框图

入数字符号为  $\{b_i\}$  时, 编码器的输出 1 为高电平, 其他输出 2、3、4 均为低电平, 由此可利用  $\{b_i\}$  对 7 涡卷混沌吸引子的斜率  $M_0^{(0)}$  进行键控。同理, 可利用数字符号  $\{b_2\}$ 、 $\{b_3\}$ 、 $\{b_4\}$  分别对 7 涡卷混沌吸引子的斜率  $M_2^{(0)}$ 、 $M_4^{(0)}$ 、 $M_6^{(0)}$  进行键控, 这样可将每个数字符号  $\{b_i (i=1, 2, 3, 4)\}$  映射到 7 涡卷混沌吸引子的各个不同的涡卷之中, 从而使发送端产生一个混沌扩频信号  $x^{(0)}(t)$ ,  $x^{(0)}(t)$  经信道传送到接收端。在接收端, 首先根据驱动-响应式同步和相关解调原理, 对接收到的信号  $x^{(0)}(t)$  和接收端的 4 个 7 涡卷混沌吸引子产生的信号  $x^{(i)}(t) (i=1, 2, 3, 4)$  分别进行相关运算。由于在接收端的 4 个 7 涡卷混沌吸引子中, 在多进制数字信号的每一个码元的持续时间  $T_b$  内, 只有其中的一个能够与发送端的 7 涡卷混沌吸引子保持同步, 其余的 3 个则处于失步状态。这样, 就可通过判决及最大值选择的原则, 将相关器的各个输出值  $\{w_i (i=1, 2, 3, 4)\}$  进行比较和判决, 选择其中最大者作为输出, 最后可在接收端恢复出原 4 进制数字序列  $\{\dots, b_1, b_3, b_2, b_4, b_3, b_1, b_4, b_2, \dots\}$ 。

### 4 MDCSK 的工作原理

首先定义门函数

$$g_i(b_i) = \begin{cases} 1 & b_i \neq 0 \\ 0 & b_i = 0 \end{cases} \quad (i = 1, 2, 3, 4) \quad (6)$$

其中, 门函数  $g_i(b_i)$  的宽度 (即多进制数字符号的码元宽度) 为  $T_b = 10\mu s$ 。

在发送端, 用 4 进制符号  $\{b_i (i=1, 2, 3, 4)\}$  对发送端 7 涡卷混沌吸引子中  $f(x^{(0)})$  的 4 个斜率值  $[M_0^{(0)}, M_2^{(0)}, M_4^{(0)}, M_6^{(0)}]$  进行参数调制, 调制后的参数可表为 (未调制参数保持不变, 即  $m_i^{(0)} = M_i^{(0)}$ )

$$\begin{aligned} & [m_0^{(0)}, m_2^{(0)}, m_4^{(0)}, m_6^{(0)}] \\ & = [M_0^{(0)} + \Delta M_0^{(0)} g_1(b_1), M_2^{(0)} + \Delta M_2^{(0)} g_2(b_2), \\ & \quad M_4^{(0)} + \Delta M_4^{(0)} g_3(b_3), M_6^{(0)} + \Delta M_6^{(0)} g_4(b_4)] \quad (7) \end{aligned}$$

式(7)中的各个参数值为

$$\begin{cases} [M_0^{(0)}, M_2^{(0)}, M_4^{(0)}, M_6^{(0)}] = [0.170, 0.380, 0.127, 0.227] \\ [\Delta M_0^{(0)}, \Delta M_2^{(0)}, \Delta M_4^{(0)}, \Delta M_6^{(0)}] = [0.01, 0.02, 0.03, 0.04] \end{cases} \quad (8)$$

其中,  $[\Delta M_0^{(0)}, \Delta M_2^{(0)}, \Delta M_4^{(0)}, \Delta M_6^{(0)}]$  为参数的调制量, 参数调制量大小的选择应适中, 仿真结果表明, 一般在  $5\% \leq |\Delta M_i^{(0)} / M_i^{(0)}| \leq 30\% (i=0, 2, 4, 6)$  之间比较合适。过大的参数调制量会使同步时间增大, 而过小的调制量将使接收端相关解调器的 4 个输出值  $w_i (i=1, 2, 3, 4)$  之间的差别变小。因此, 过大或过小的调制量将不利于在接收端对输出数字信号的判决。

在接收端, 4 个 7 涡卷混沌吸引子相应的调制参数可表为如下的矩阵形式

$$\begin{bmatrix} m_0^{(1)} & m_2^{(1)} & m_4^{(1)} & m_6^{(1)} \\ m_0^{(2)} & m_2^{(2)} & m_4^{(2)} & m_6^{(2)} \\ m_0^{(3)} & m_2^{(3)} & m_4^{(3)} & m_6^{(3)} \\ m_0^{(4)} & m_2^{(4)} & m_4^{(4)} & m_6^{(4)} \end{bmatrix} = \begin{bmatrix} M_0^{(1)} + \Delta M_0^{(1)} & M_2^{(1)} & M_4^{(1)} & M_6^{(1)} \\ M_0^{(2)} & M_2^{(2)} + \Delta M_2^{(2)} & M_4^{(2)} & M_6^{(2)} \\ M_0^{(3)} & M_2^{(3)} & M_4^{(3)} + \Delta M_4^{(3)} & M_6^{(3)} \\ M_0^{(4)} & M_2^{(4)} & M_4^{(4)} & M_6^{(4)} + \Delta M_6^{(4)} \end{bmatrix} \quad (9)$$

式中,  $[m_0^{(1)}, m_2^{(1)}, m_4^{(1)}, m_6^{(1)}]$ 、 $[m_0^{(2)}, m_2^{(2)}, m_4^{(2)}, m_6^{(2)}]$ 、 $[m_0^{(3)}, m_2^{(3)}, m_4^{(3)}, m_6^{(3)}]$ 、 $[m_0^{(4)}, m_2^{(4)}, m_4^{(4)}, m_6^{(4)}]$  分别为接收端 4 个 7 涡卷混沌吸引子相应的调制参数。对于未调制的参数则保持原来的值不变, 即  $m_i^{(k)} = M_i^{(k)}$ 。在上述条件下, 当发送端发送数字符号  $\{b_i (i=1, 2, 3, 4)\}$  时, 可分别使接收端的第  $i (i=1, 2, 3, 4)$  个 7 涡卷混沌吸引子保持同步, 而其他标号不一致的 7 涡卷混沌吸引子则处于失步状态, 因此, 在接收端按相关解调原理及最大值选择输出可将相对应的数字符号  $\{(b_i (i=1, 2, 3, 4))\}$  正确地解调出来。

经多进制数字符号  $\{b_i (i=1, 2, 3, 4)\}$  调制后, 发送端 7 涡卷混沌吸引子的状态方程为

$$\begin{cases} dx^{(0)}/d\tau = \alpha[y^{(0)} - f(x^{(0)})] \\ dy^{(0)}/d\tau = x^{(0)} - y^{(0)} + z^{(0)} \\ dz^{(0)}/d\tau = -\beta y^{(0)} \end{cases} \quad (10)$$

$$\begin{cases} dx^{(i)}/d\tau = \alpha[y^{(i)} - f(x^{(i)})] \\ dy^{(i)}/d\tau = x^{(0)} - y^{(i)} + z^{(i)} \\ dz^{(i)}/d\tau = -\beta y^{(i)} \end{cases} \quad (i=1,2,3,4) \quad (11)$$

发送端输出经多进制数字符号  $\{b_i (i=1,2,3,4)\}$  调制后的 7 涡卷混沌扩频信号  $x^{(0)}(t)$ 。 $x^{(0)}(t)$  经信道传至接收端,利用  $x^{(0)}(t)$  分别对接收端的 4 个 4 涡卷混沌吸引子实现驱动-响应式同步。接收端 4 个 7 涡卷混沌吸引子的状态方程均可表为如下的统一形式

式中,标号  $i=1,2,3,4$  分别代表接收端 4 个 7 涡卷混沌吸引子所对应的状态方程, $x^{(0)}$  为驱动信号,  $[x^{(i)}, y^{(i)}, z^{(i)}] (i=1,2,3,4)$  分别为接收端 4 个 7 涡卷混沌吸引子相应的状态变量。式(10)和式(11)中各个分段线性函数  $f(x^{(l)}) (l=0,1,2,3,4)$  可统一表示为

$$f(x^{(l)}) = m_{N-1}^{(l)} x^{(l)} + 0.5 \sum_{i=1}^{N-1} (m_{i-1}^{(l)} - m_i^{(l)}) \cdot (|x^{(l)} + x_i^{(l)}| - |x^{(l)} - x_i^{(l)}|)$$

$$= \begin{cases} m_0^{(l)} x^{(l)} & (|x^{(l)}| < x_1^{(l)}) \\ m_i^{(l)} x^{(l)} + \sum_{j=1}^i (m_{j-1}^{(l)} - m_j^{(l)}) x_j^{(l)} \cdot \frac{|x^{(l)}|}{x^{(l)}} & (x_i^{(l)} \leq |x^{(l)}| < x_{i+1}^{(l)}, i=1,2,\dots,N-2) \\ m_{N-1}^{(l)} x^{(l)} + \sum_{j=1}^{N-1} (m_{j-1}^{(l)} - m_j^{(l)}) x_j^{(l)} \cdot \frac{|x^{(l)}|}{x^{(l)}} & (|x^{(l)}| > x_{N-1}^{(l)}) \end{cases} \quad (12)$$

可用以下的递推公式来确定  $x_i^{(l)} (i=2,3,\dots,N-1, l=0,1,2,3,4)$

### 5 相关解调、判决及最大值选择输出

$$\begin{cases} x_2^{(l)} = \frac{2 \sum_{i=1}^1 (m_i^{(l)} - m_{i-1}^{(l)}) x_i^{(l)}}{m_1^{(l)}} - x_1^{(l)} \\ x_3^{(l)} = \frac{2 \sum_{i=1}^2 (m_i^{(l)} - m_{i-1}^{(l)}) x_i^{(l)}}{m_2^{(l)}} - x_2^{(l)} \\ \dots\dots \\ x_{N-2}^{(l)} = \frac{2 \sum_{i=1}^{N-3} (m_i^{(l)} - m_{i-1}^{(l)}) x_i^{(l)}}{m_{N-3}^{(l)}} - x_{N-3}^{(l)} \\ x_{N-1}^{(l)} = \frac{2 \sum_{i=1}^{N-2} (m_i^{(l)} - m_{i-1}^{(l)}) x_i^{(l)}}{m_{N-2}^{(l)}} - x_{N-2}^{(l)} \end{cases} \quad (13)$$

混沌信号是具有遍历性的宽带非周期信号。其自相关和互相关具有类噪声一样的冲击相关特性,其自相关和互相关函数可由下式计算获得

$$\begin{cases} R_{x^{(0)}x^{(0)}}(\tau) = \frac{1}{T_b} \int_{T_b} x^{(0)}(t) x^{(0)}(t - \tau) dt \\ R_{x^{(0)}x^{(i)}}(\tau) = \frac{1}{T_b} \int_{T_b} x^{(0)}(t) x^{(i)}(t - \tau) dt \end{cases} \quad (14)$$

在没有受到输入信号  $S_{in}(t)$  调制时,发送端 7 涡卷混沌吸引子分段线性函数  $f(x^{(0)})$  中的斜率  $M_i^{(0)}$  和转折点  $X_i^{(0)}$  为固定值,由式(3)和式(4)确定。当受到  $S_{in}(t)$  调制后, $f(x^{(0)})$  中的调制参数  $m_i^{(0)}$  和  $x_i^{(0)}$  均受  $S_{in}(t)$  的调制而动态地离散变化,可由式(7)和式(13)确定其动态瞬时离散值  $m_i^{(0)}$  和  $x_i^{(0)}$ 。当出现数字符号  $\{b_i (i=1,2,3,4)\}$  时,相应的  $g_i(b_i)=1$ ,发送端吸引子的调制参数和接收端相对应的第  $i (i=1,2,3,4)$  个吸引子的调制参数匹配,而接收端其他标号不一致的混沌吸引子的调制参数则处于失配状态。因此,可用相关解调的方法恢复出原数字序列。

混沌信号是具有遍历性的宽带非周期信号。其自相关和互相关具有类噪声一样的冲击相关特性,其自相关和互相关函数可由下式计算获得

对于收发两端同步的混沌信号,有  $x^{(0)}(t) = x^{(i)}(t) (i=1,2,3,4)$ ,它们具有完全的相关性,而对于不同步的混沌信号,有  $x^{(0)}(t) \neq x^{(i)}(t) (i=1,2,3,4)$ ,则其相关性很弱,由此可用相关检测的方法恢复出原信号。定义相关系数为  $\rho = \int_{T_b} x^{(0)}(t) x^{(i)}(t) dt / E_b$ ,其中  $E_b$  为信号的比特能量,对于发送端和接收端同步的两个混沌信号,有  $\rho_{x^{(0)}x^{(i)}} = \rho_{x^{(i)}x^{(0)}} = 1 (i=1,2,3,4)$ ,对于发送端和接收端不同步的两个混沌信号,则  $\rho_{x^{(0)}x^{(i)}} \approx 0 (i=1,2,3,4)$ 。在图 4 中,可得相关解调器的各个输出为

$$w_i = \int_{T_b} x^{(0)}(t) x^{(i)}(t) dt = \begin{cases} \int_{T_b} x^{(0)}(t) x^{(0)}(t) dt = \rho_{x^{(0)}x^{(0)}} E_b & b_i \neq 0 \\ \int_{T_b} x^{(0)}(t) x^{(i)}(t) dt = \rho_{x^{(0)}x^{(i)}} E_b & b_i = 0 \end{cases} \quad (i=1,2,3,4) \quad (15)$$

接收端的判决及最大值选择输出可由下式决定

$$S_{out} = \max\{w_1, w_2, w_3, w_4\} \quad (16)$$

### 6 计算机模拟结果

用 4 进制数字序列  $\{\dots b_1, b_4, b_2, b_3, b_4, b_3, b_1, b_4, b_2, \dots\}$

$b_2, \dots\}$  对所提出的方案进行了计算机模拟, 模拟结果如图 5 所示。若收发两端混沌吸引子同步时, 误差信号为 0, 失步时, 误差信号不为 0, 根据式 (14)~(16), 可通过相关解调和最大值选择输出的方法将原 4 进制数字序列  $\{\dots b_1, b_4, b_2, b_3, b_4, b_3, b_1, b_2, \dots\}$  解调出来。限于篇幅, 这里没有给出有关接收端 7 涡

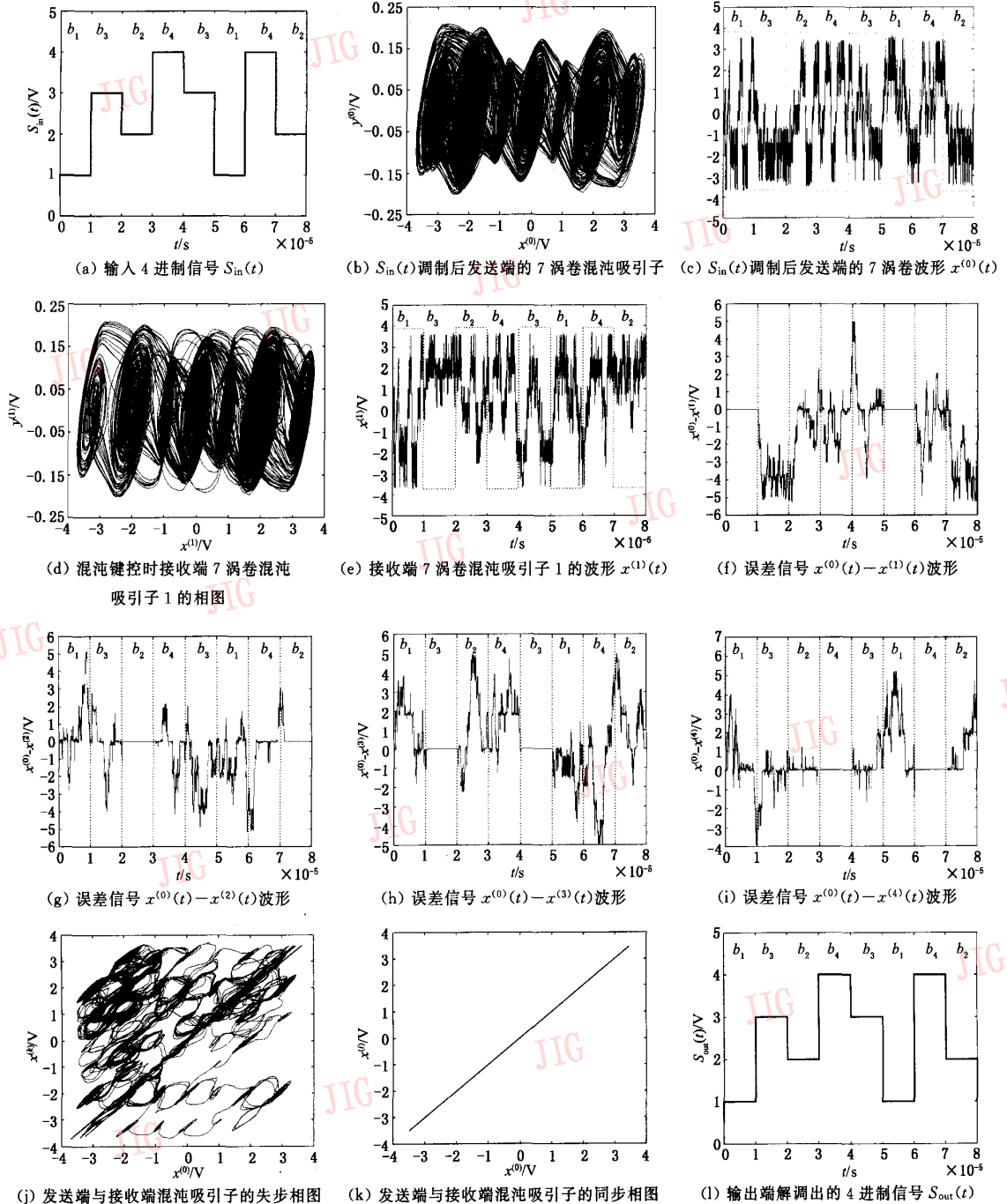


图 5 多进制数字混沌键控(MDCSK)的计算机模拟结果

卷混沌吸引子 2、3、4 各自的相图以及它们混沌输出波形  $x^{(i)}(t)$  ( $i=2,3,4$ ), 这些混沌吸引子的相图及输出波形与 7 涡卷混沌吸引子 1 的相图及输出波形在形式上是类似的。此外, 根据式(10)和式(11), 图 5 中的各时域波形还考虑了时间尺度变换  $\tau=t/\tau_0$  的情况, 其中, 时间尺度变换因子为  $\tau_0=2.0 \times 10^{-8}$  s。

## 7 结 论

基于多涡卷混沌系统的多进制数字混沌键控 (MDCSK) 新方案, 是文献[3]所提出的二进制混沌键控 (CSK) 方法的扩充和推广。在该方案中, 利用多进制数字信号对发送端多涡卷混沌吸引子中各个涡卷的大小与形状进行调制, 从而可将每个数字符号  $\{b_i (i=1,2,3,4)\}$  映射到 7 涡卷混沌吸引子的各个不同的涡卷之中, 使发送端产生一个混沌扩频信号。在接收端, 根据驱动-响应式同步与相关解调原理恢复出原多进制数字序列。与文献[3]所提出的二进制混沌键控相比, 多进制混沌键控的两个特点是:

(1) 由于  $N$  涡卷混沌吸引子中的分段线性函数  $g(\cdot)$  可具有  $N$  个不同的斜率, 因此, 它既能能传递二进制数字信号, 又能传递多进制数字信号, 而在采用双涡卷混沌吸引子的 CSK 系统中, 由于其分段线性函数  $f(x)$  只有两个不同的斜率, 一般只适合传递二进制数字信号, 而对传递多进制数字信号时就显得所需调制的参数(如斜率)不够;

(2) 由于采用了混沌动力学行为更复杂以及密钥参数更多的多涡卷混沌信号进行扩频, 这一方案具有更好的保密性能, 在事先不知道各混沌参数和调制量大小的情况下, 要想破译原数字序列有较大的难度。

## 参 考 文 献

- Kolumban G, Kennedy M P, Chua L O. The role of synchronization in digital communications using chaos-Part II: Chaotic modulation and chaotic synchronization [J]. IEEE Transactions on Circuits and Systems-I, 1998, 45(11): 1129~1140.
- Kolumban G, Kennedy M P. The role of synchronization in digital communications using chaos-Part 3: Performance bounds for correlation receivers[J]. IEEE Transactions on Circuits and Systems-I, 2000, 47(12): 1673~1683.
- Dedieu H, Kennedy M P, Hasler M. Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits[J]. IEEE Transactions on Circuits and Systems-II, 1993, 40(10): 634~643.
- Kennedy M P, Kolumban G, Kis G, et al. Performance evaluation of FM-DCSK modulation in multipath environments [J]. IEEE Transactions on Circuits and Systems-I, 2000, 47(12): 1702~1711.
- Kolumban G, Kennedy M P, Kis G, et al. FM-DCSK: A robust modulation scheme for chaotic communications [J]. IEICE Transactions Fundamentals, 1998, E81-A(9): 1798~1802.
- Yang T, Chua L O. Chaotic digital code-division multiple access (CDMA) communication systems [J]. International Journal of Bifurcation and Chaos, 1997, 7(12): 2789~2805.
- Matsumoto T, Chua L O, Komuro M. The double scroll [J]. IEEE Transactions on Circuits and Systems-I, 1985, 32(8): 798~817.
- Chua L O, Komuro M, Matsumoto T. The double scroll family, Part 1 and Part 2 [J]. IEEE Transactions on Circuits and Systems-I, 1986, 33(11): 1073~1118.
- Zhong G Q, Ayrom F. Experimental confirmation of chaos from Chua's circuit [J]. International Journal of Circuit Theory and Applications, 1985, 13(1): 93~98.
- Suykens J A K, Vandewalle J. Generation of  $n$ -double scrolls ( $n=1,2,3,4,\dots$ ) [J]. IEEE Transactions on Circuits and Systems-I, 1993, 40(11): 861~867.
- Yalcin M E, Suykens J A K, Vandewalle J. Experimental confirmation of 3- and 5-scroll attractors from a generalized Chua's circuit [J]. IEEE Transactions on Circuits and Systems-I, 2000, 47(3): 425~429.
- 禹思敏, 丘水生, 林清华. 多涡卷混沌吸引子研究的新结果 [J]. 中国科学(E 辑), 2003, 33(4): 365~374.
- Tang W K S, Zhong G Q, Chen G, et al. Generation of  $N$ -scroll attractors via sine function [J]. IEEE Transactions on Circuits and Systems-I, 2001, 48(11): 1369~1372.
- Pecora L M, Carroll T L. Synchronization in chaotic systems [J]. Physical Review Letters, 1990, 64(8): 821~823.

禹思敏 1957 年生。教授。2001 年于华南理工大学电子与信息学院获电路与系统专业博士学位, 现分别在广东工业大学信息工程学院和自动化学院任教。目前主要从事混沌理论与保密通信、通信理论与技术、数字电视与高清晰度电视等方面的教学与科研工作。



E-mail: siminyu@21cn.com

林清华 1956 年生。副教授。1982 年于湖南师范大学(原湖南师范学院)物理系获物理专业学士学位, 1986 年毕业于厦门大学物理系研究生班。研究方向为凝聚态物理。目前主要从事凝聚态物理、非线性光学、混沌理论等方面的教学与科研工作。

丘水生 1939 年生。教授、博士生导师。1966 年于华南工学院非线性振荡理论专业研究生毕业。1984~1986 年为加拿大阿尔伯特大学访问学者, 1990~1991 年先后为美国波特兰州立大学、加拿大阿尔伯特大学访问教授。目前从事非线性电路与功率电子学、混沌理论与保密通信等方面的教学与科研工作。