保密通信中数字流混沌产生器的同步

赵 耿[1],郑德玲[2]
(1. 北京科技大学信息工程学院,北京 100083 2. 北京电子科技学院科研中心,北京,100070)

摘 要: 由于混沌保密通信系统研究中传统的连续流混沌同步理论存在一些难于解决的问题,本文提出了基于数字流混沌的混沌保密通信理论,在实验室中实现了一类语音保密通信方案,建立了数字流混沌产生器的时钟间隔脉冲驱动同步原理和实现方法,同步通信实验表明,该方法是可行的.

关键词: 数字流混沌同步; 时钟间隔脉冲驱动; 同步噪声
中图分类号: *TN*901 **文献标识码**: *A* **文章编号**: 0372-2112 (2002) 04-0536-04

Synchronization of Digital-Flow Chaos Generators in Secure Communication

ZHAO Geng[1], ZHENG De-ling[2]
(1. *Information Engineering School, UST, Beijing, Beijing* 100083, *China*
2. *Science rearch center, Beijing Electrical Science and Technology Institute, Beijing* 100070, *China*)

Abstract: In secure communications, it is difficult to solve some existing problems of conventional synchronization between two continuous-flow chaotic systems. Therefore, in this paper the theorems on synchronization based on digital-flow chaos in secure communications are presented and a scheme of secure speech communication are presented and realized. In the scheme a new synchronic method ——cycles and interval pulse drive is developed and realized. Experimental results show it is feasible.

Key words: digital-flow chaos synchronization; cycles and interval pulses drive; synchronization noise

1 引言

对初值的极其敏感性使人们一度认为混沌的同步几乎不可能,直到美国海军实验室的 L M Pecora 和 T L Carrol 发现二个混沌电路之间的自同步特性,对混沌同步问题的研究才如雨后春笋. 众多学者对混沌同步问题进行了深入的研究,提出了不少方法. 主要有连续流混沌系统中的驱动响应[1,2]、外部噪声注入[3]、相互耦合同步[4,5]、主动被动[6,7](又称有源无源分拆 APD)、连续变量反馈[8]、自适应控制[9,10]等同步方法. 混沌系统之间的同步不但具有理论意义,而且在应用中涉及到诸多领域,其特殊的应用之一就是同步保密通信. 对保密通信而言,主要研究的是驱动响应、主动被动法及相互耦合同步法.

驱动响应同步是近似同步,信息信号恢复精度不高;受到系统特定分解的限制,能作此分解的系统并不多;小的信息信号功率使保密通信易遭受相空间重构、回归映射等法的攻击,且信噪比低[3];在信道噪声的影响下,有可能同步难以建立,因而难于实用. 主动被动同步需要采取恰当的技术减少信息信号的误差、减少噪声的影响及从 s 中提取所需信息[3];并且,这种方法也要求一个稳定的同步区,信号可能被信道噪声扭曲从而偏离该同步区,导致无法同步;另外,若信息信号幅值太高,接收机和发射机方的奇怪吸引子可能被打破,这些问题尚有待深入研究和解决. 相互耦合同步虽然也得到较多的研究,但由于需要选取合适的耦和变量,能找到这种变量的混沌系统并不多,目前主要集中在对 Chua's 电路的研究上.

然而到目前为止,绝大多数的混沌保密通信研究尚仅限于理论研究和仿真阶段(包括所作的实验),因此本文针对我们研究并实现了的基于数字流混沌产生器的双工语音保密通信系统,建立了数字流混沌同步的理论,提出了时钟间隔脉冲驱动同步法,给出了数字流混沌产生器的同步定义和同步定理. 并给出了实验结果,旨在能把混沌保密通信用于真正的实际系统中去.

2 数字流混沌同步定义

文献[11][12]指出用数字混沌产生器代替连续流混沌产生器便于控制和实现且保密性强,只是目前实用的同步方法较少. 数字流混沌是在数字混沌的基础上提出的,在此先给出数字流混沌及数字流混沌同步的概念.

定义 1 设有一离散数字迭代系统

$$x(k+1) = F(x(k)) \tag{1}$$

其中,$k = g(t_{xk})$, $k \in IR^+$, $t_{xk} \in R$,若对任意时刻 t, $t \in [t_{xk}, t_{x(k+1)}]$有

$$x(t) = x(k) + \frac{x(k+1) - x(k)}{t_{x(k+1)} - t_{xk}}(t - t_{xk}) \tag{2}$$

收稿日期:2000-11-24;修回日期:2001-07-06
基金项目:国家自然科学基金(No. 69772014)

则称 $x(t)$ 为数字流混沌.

定义 2　设有二个离散数字迭代混沌系统

$$\text{系统 1}\qquad x(k+1)=F(x(k)) \tag{3}$$

$$\text{系统 2}\qquad y(\bar{k}+1)=F(y(\bar{k})) \tag{4}$$

其中:$x(k)=\{x_1(k),x_2(k),\cdots,x_n(k)\}^T$, $y(\bar{k})=\{y_1(\bar{k}),y_2(\bar{k}),\cdots,y_n(\bar{k})\}^T$, $k=g(t_{xk})$, $\bar{k}=g(t_{y\bar{k}})$, $x(k)$, $y(\bar{k})\in R^n$, $k,\bar{k}\in IR^+$, $t_x,t_y\in R$ 分别为 $F(x(k))$, $F(y(\bar{k}))$ 第 k 次和第 $\bar{k}$ 次迭代点时间,如果对 $t_{xk}\to t_{y\bar{k}}$,有

$$\|x(k)-y(\bar{k})\|\le e^{-\alpha}\|x(0)-y(0)\| \quad (\alpha\text{为指数同步率}) \tag{5}$$

或对任意初始条件

$$\|x(k+1)-y(\bar{k}+1)\|\le e^{-\alpha}\|x(j)-y(j)\|,\quad j<\min\{(k+1),(\bar{k}+1)\}$$

则称二个离散数字系统渐进同步,若 $t_{xk}=t_{y\bar{k}}$ 恒有

$$\|x(k)-y(k)\|\equiv 0 \tag{6}$$

则称二个离散数字系统立即同步.

定义 3　设有二个数字流混沌系统

$$\text{系统 1}\quad\begin{cases}x(k+1)=F(x(k))\\ x(t)=x(k)+\dfrac{x(k+1)-x(k)}{t_{x(k+1)}-t_{xk}}(t-t_{xk})\end{cases} \tag{7}$$

$$\text{系统 2}\quad\begin{cases}y(\bar{k}+1)=F(y(\bar{k}))\\ y(t)=y(\bar{k})+\dfrac{y(\bar{k}+1)-y(\bar{k})}{t_{y(\bar{k}+1)}-t_{y\bar{k}}}(t-t_{y\bar{k}})\end{cases} \tag{8}$$

如果系统 1 和系统 2 中 $x(k+1)$, $y(\bar{k}+1)$ 满足定义 2 下的渐进同步或立即同步,则称系统 1 和系统 2 渐进同步或立即同步.

对数字流混沌保密通信系统而言,立即同步更具有实际意义,但这要求 $t_{xk}=t_{y\bar{k}}$,即二个系统的迭代次数在时间上保持一致同步,也即二个离散数字系统每次迭代需要的时间相等.然而实验表明,二个离散数字系统中每一方智能芯片的每迭代一次的时间是不等间隔的,它们是系统映射参数 μ_x, μ_y, 及初值 $x(0)$、$y(0)$,时钟周期 T_x、T_y 的函数.设二个离散数字系统每次迭代所需时间 T_{xi}、T_{yi}, $i\in IR^+$ 组成的集合为 U、V.则

$$U=\{f_1(\mu_x,x(0),T_x),f_2(\mu_x,x(0),T_x),\cdots,f_\infty(\mu_x,x(0),T_x)\}$$
$$V=\{f_1(\mu_y,y(0),T_y),f_2(\mu_y,y(0),T_y),\cdots,f_\infty(\mu_y,y(0),T_y)\} \tag{9}$$

有定理 1 成立.

定理 1　对二个 n 维数字混沌迭代系统,若 μ_x、μ_y 为系统映射参数向量, $x(0)$, $y(0)\in R^n$, $T_x\in U$, $T_y\in V$,保证二个系统立即同步的充分必要条件是:$\mu_x=\mu_y$, $x(0)=y(0)$, $T_x=T_y$.

证:显然.略.

3　数字流混沌产生器同步的实现

时钟——间隔脉冲驱动同步原理:对于参数及初始值严格一致的二个相同混沌迭代系统,若保证时钟 $T_x=T_y$,使其满足定理 1,理论上已可实现立即同步,但实际上,为了保证二个混沌系统是相同的,对智能芯片的编程还必需完全一致.由于收发方总有一些各自不同的条件判断和控制(这也正是数字流混沌便于实用的原因),这一点也难做到.另外,若非可调时钟, $T_x=T_y$ 也难精确保证.为此,引入间隔脉冲驱动 $\zeta(k/N)$ 以减少同步误差.图 1 所示为一维单向同步的 Logistic 映射数字流混沌遮掩保密通信系统发射方和接收方方框图.

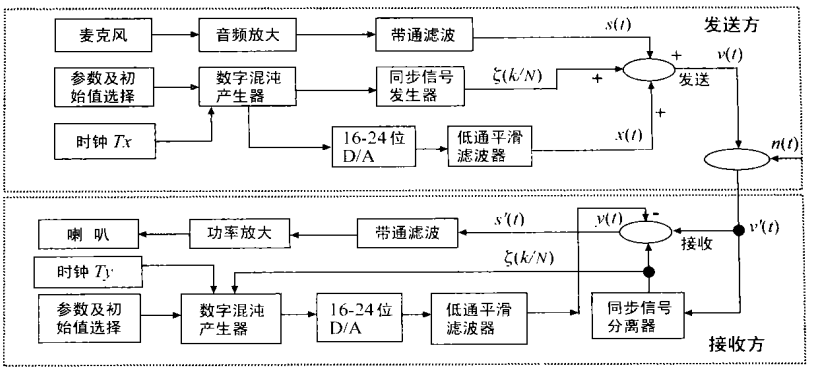


图 1　单向同步数字流混沌遮掩保密通信系统发射方和接收方方框图

图 2 所示为无间隔脉冲驱动下,二个相同的数字流混沌系统的混沌信号 1、3,及其同步误差 2 随时间的变化情况.图 3 所示为图 2 中混沌信号 1、3 同步的李沙育图形.从图 2 中能看出同步误差随时间增加而增加,即同步误差随时间增加呈发散态,从图 3 中也能看出同步效果变差.

同步误差随时间增加呈发散态,意味着信息信号最终被淹没在一片噪声中.在图 1 系统中引入间隔脉冲驱动 $\zeta(k/N)$ 后:

发送方:$v(t)=x(t)+v(t)+\zeta(k/N)$ (10)

接收方:$s'(t)=v'(t)-y(t)-\zeta'(k/N)$ (11)

其中:$x(t)=f(x(k))$, $y(t)=f(y(k))$, $v'(t)=v(t)+n(t)$, $n(t)$ 为信道噪声, $\zeta(k/N)=\zeta'(k/N)$.

$$\zeta(k/N)=\begin{cases}C\cdot\delta(m), & \text{when}\quad m=k/N,\ N\ne 1,\ m\in IR^+,\ k=g(t)\\ 0, & \text{else}\end{cases} \tag{12}$$

式中:C 为一电路常数, N 为非 1 正整数, $f(\cdot)$ 为 D/A 转换及低通平滑滤波的单值非线性函数, $\delta(m)$ 为脉冲函数.因此可认为 $\zeta(k/N)$ 为间隔脉冲驱动函数,当 $(m-1)\cdot N<k<m\cdot N$ 时,依靠发送方和接收方精确的时钟来保证同步.当 $k=m\cdot N$ 时由间隔脉冲驱动同步,所以称时钟间隔脉冲驱动同步.

图 4 为时钟间隔脉冲驱动同步测试图.图 4(a) 中(1)、(2)为二个同步的混沌信号,(3)、(4)为同步误差曲线,为了清楚观察间隔脉冲驱动的作用,图中保留并放大了间隔脉冲.图 4(b) 中(1)为原始语音信号,(2)为混沌载波信号,(3)为混沌信号,(4)为恢复语音信号.显然,在未进行间隔脉冲驱动的前半部分,含有同步噪声,在间隔脉冲驱动同步后,同步噪声很小.

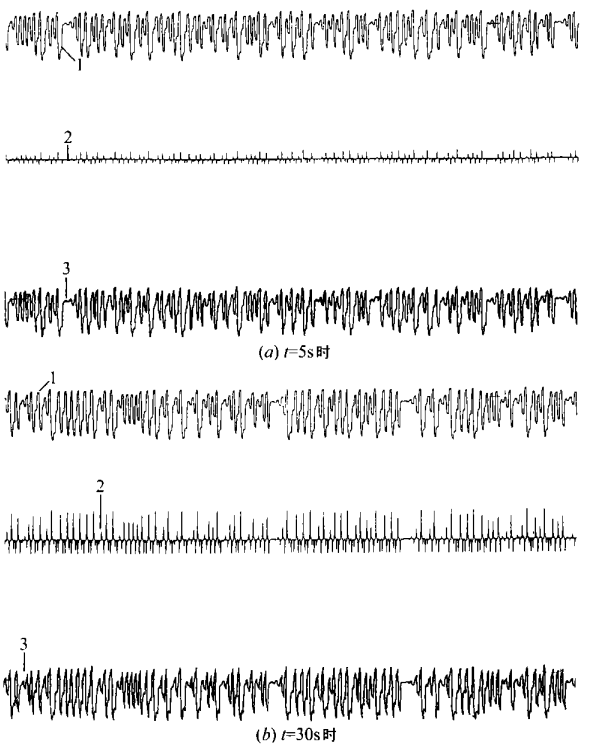


图 2 混沌同步及同步误差随时间变化的曲线

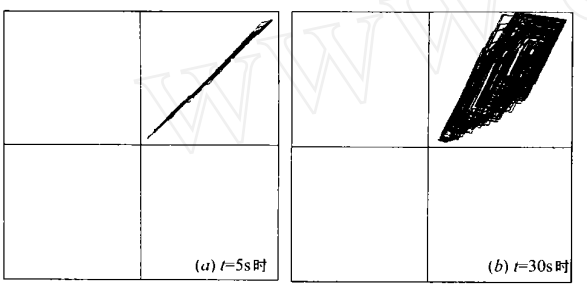


图 3 二个混沌系统输出同步的李沙育图形

实验表明,若数字流混沌映射器由电路实现[13](如非线性数字滤波器)需收发方电路系统参数精确一致(这是不可能的),即要求本文智能芯片的程序严格一致(可以做到).这正是保密通信对电路参数及初值敏感性所要求的,本文系统中数字流混沌映射器为智能芯片 89C52,时钟晶振为 24MHz. ,曲线由德国造 Hioki8840 MEMORY Hicorder 八笔高速记录仪记录.

4 时钟间隔脉冲驱动同步定理

由于定理 1 的条件 $T_x = T_y$ 难于精确满足,采用时钟间隔脉冲驱动同步法,旨在阻止二系统失步,设 t_{xk}, t_{yk} 为二系统第 k 次迭代点时的时间,有: $t_{xk} = \sum_{i=1}^{k} T_{xi}$, $t_{yk} = \sum_{i=1}^{k} T_{yi}$, $T_{xk} \in U$, $T_{yi} \in V$. 为了确定时钟间隔脉冲驱动同步的有效条件,先定义失步的概念.

定义 4 二个混沌迭代系统 $F(x(k))$, $F(y(\bar{k}))$,在时域上若存在一个时间点使得二个系统同时开始的迭代次 $|k - \bar{k}| \geq 1$,或者说不同时开始的迭代次 $|k - \bar{k}| \geq 2$,称二系统失步. 此时必有 $t_{xk} \geq t_{y(k+1)}$ 或 $t_{y\bar{k}} \geq t_{x(\bar{k}+1)}$.

那么,为保证二系统不失步,有定理 2,定理 3 成立.

定理 2 对二个混沌迭代系统 $F(x(k))$, $F(y(\bar{k}))$,其每次迭代时间 T_{xi}、T_{yi} 所组成的集合为 U、V 最小迭代时间 $T_{\min} = \min\{U \cup V\}$, $T_{xi} \in U$, $T_{yi} \in V$,不失步的充分条件是:对任意的 N, $N \in IR^{+}$ 使得 $\left|\sum_{i=1}^{N}(T_{xi} - T_{yi})\right| < T_{\min}$.

证: 由于 $\left|\sum_{i=1}^{N}(T_{xi} - T_{yi})\right| < T_{\min}$

当 $\sum_{i=1}^{N}(T_{xi} - T_{yi}) > 0$ 时, $\sum_{i=1}^{N}(T_{xi} - T_{yi}) < T_{\min}$

又因 $T_{x(N+1)} \in \{U \cup V\}$,必有 $\sum_{i=1}^{N}(T_{xi} - T_{yi}) < T_{x(N+1)}$,即

$$\sum_{i=1}^{N} T_{xi} < \sum_{i=1}^{N} T_{yi} + T_{y(N+1)} = \sum_{i=1}^{N+1} T yi$$

从而由定义 2 知(不同时迭代),必有 $k - \bar{k} < 2$. 同理可证当 $\sum_{i=1}^{N}(T_{xi} - T_{yi}) < 0$ 时, $\bar{k} - k < 2$,从而对任意的 N 若使 $\left|\sum_{i=1}^{N}(T_{xi} - T_{yi})\right| < T_{\min}$,必可保证二混沌迭代系统不失步.

定理 3 对二个混沌迭代系统 $F(x(k))$, $F(y(\bar{k}))$,其每次迭代时间 T_{xi}、T_{yi} 所组成的集合为 U、V,最小迭代时间 $T_{\min} = \min\{U \cup V\}$,最大迭代时间 $T_{\max} = \max\{U \cup V\}$, $T_{xi} \in U$, $T_{yi} \in V$ 为保证二系统不失步, N 值的选择需满足 $N < T_{\min}/(T_{\max} - T_{\min})$

证:设 $F(x(k))$ 迭代第 N 次时与 $F(y(\bar{k}))$ 失步,则有:

$$N \cdot T_{\max} \geq \sum_{i=1}^{N} T_{xi} \geq \sum_{i=1}^{N+1} T_{yi} \geq (N+1) \cdot T_{\min}$$

即 $N \cdot T_{\max} \geq (N+1) \cdot T_{\min}$, $N \geq T_{\min}/(T_{\max} - T_{\min})$

上述定理只保证了时钟间隔脉冲驱动同步不失步的条件,由于实际过程中 $N = 1$ 难于实现且保密性不强,还要求 $N > 1$,同时还应考虑通信信噪比大于 20dB,以满足语音通信要求. 本文系统中取 $N = 500$.

5 时钟间隔脉冲驱动同步的特点

由上所述可知,时钟间隔脉冲驱动有如下特点.

(1) 本文数字流混沌同步属立即同步 $t_h = 0$,响应时间快.

(2) 时钟间隔脉冲驱动同步也属精确同步,而精确同步的信噪比高.

(3) 数字混沌可按需求增大信息信号幅度,因而信噪比高,同时使传统的对混沌遮掩通信的攻击方法难以奏效,保密性强.

(4) 要求发送方的参考模型混沌产生器和接收方的混沌产生器软件和初始条件一致,由相同的软件可精确保证一致性,这正是保密通信保密性所需要的.

(5) 数字流混沌产生器不存在混沌系统分拆问题,因而可用的混沌模型可足够多,使用高维混沌更容易.

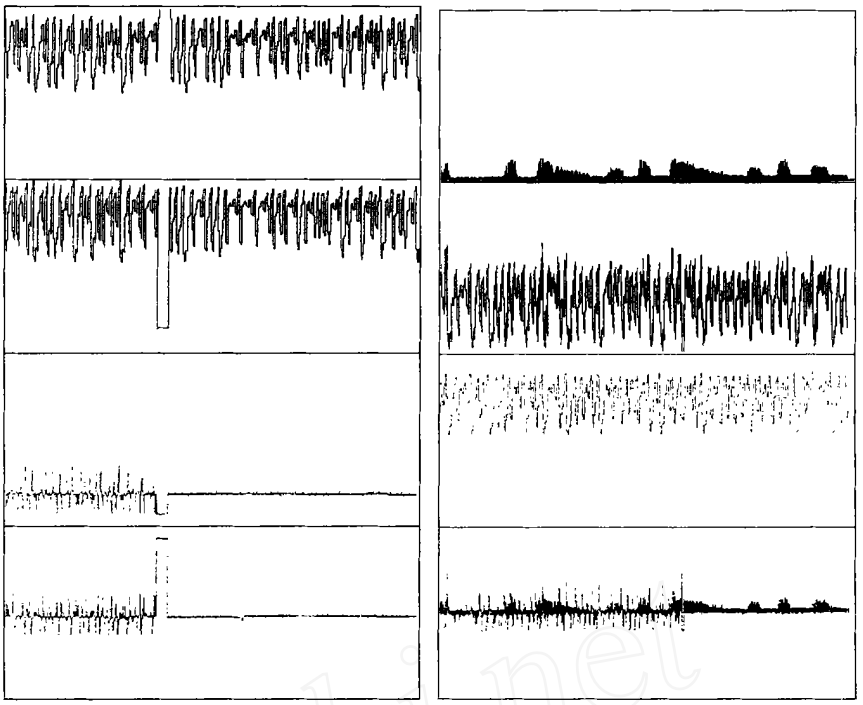
(6)数字流混沌产生器很容易改变系统参数及初始条件,可控性好.

(7)数字流混沌产生器的同步仍保留了原混沌系统宽带类噪声特性,却大大减少原混沌系统的动力学特征,这也是使传统的对混沌遮掩通信的攻击方法难以奏效的原因,从而使保密性增强[14].

(8)混沌的传统同步法电路简单、元件少.而数字流混沌产生器电路相对复杂,元件多一些.另外还要求能高速运行的智能芯片 89C52 仅能完成简单的迭代速度要求,这是其缺点.

6　结论

本文研究并提出的数字流混沌产生器的时钟间隔脉冲驱动同步法已完成了实验室样机实验,在 20m 内实现了可靠的通信,但是在时钟间隔期间有噪声随时间增大的现象,为此又提出了模型参考同步去噪法,较好地消除了噪声.本文方法在小局域范围内作成实际保密通信系统是可行的,若用光纤传输将会有更好的效果.在大范围内、远距离的通信尚有待进一步的研究.



(a)不带语音时　　(b)带语音时

图 4　时钟间隔脉冲驱动同步实验

参考文献:

[1] Pecora L M,Carrol TL. Synchronization in chaos system [J]. Phy Rev, 1990,64(8):821 - 824.

[2] Pecora L M,Carrol TL. Driving systems with chaotic signals [J]. Phys Rev,1991,44(4):2374 - 2383.

[3] 方锦清.非线性系统中混沌控制方法同步原理及其应用前景[J].物理学进展,1996,16(2):137 - 202.

[4] Wu C W,Chua L O. A simple way to synchronize chaotic systems with applications to secure communication systems [J]. Int J Bifur & Chaos, 1994,6(3):1687 - 1695.

[5] Wu C W,Chua L O. Synchronization in an array of linearly coupled dynamical systems [J]. IEEE Trans on CAS,1995,42(8):430 - 447.

[6] 李国辉,徐德明,周世平.用 APD 法及主动—间隙耦合实现混沌同步[J].应用科学学报,2001,19(1):1 - 4.

[7] Wang Jinlan,Chen Guangzhi,et al. Synchronizing spatiotemporal chaos in coupled map lattices via active-passive decomposition [J]. Phys Rev E,1998,58(3):3017 - 3021.

[8] Ana Guedes de Oliverira. Synchronization of chaotic maps by feedback control and application to secure communications using chaotic neural networks [J]. Int J Bifur & Chaos,1998,8(11):2225 - 2237.

[9] Maybhate A,Amritkar R E. Use of synchronization and adaptive control in parameter estimation from a time series [J]. Phys Rev E,1999,59(1):284 - 293.

[10] Wu C W,et al. On adaptive synchronization and control of nonlinear dynamical systems [J]. Int J Bifur & Chaos,1996,6(3):455 - 461.

[11] 王可人,薛磊,等.混沌 DS 通信的一种实现方法[J].中国人民解放军电子工程学院学报,1997,7(1):13 - 19.

[12] Frey D R,Chaotic digital encoding:An approach to secure communication [J]. IEEE Trans On CAS,1993,40(10):660 - 666.

[13] 周红,罗杰,等.关于数字混沌系统保密通信系统的探讨[J].电子科学学刊,1997,19(2):202 - 207.

[14] 李克,裴文江,等.一种混沌数字保密通信系统的保密性能分析[J].电路与系统学报,1999,4(2):96 - 101.

作者简介:

赵　耿　男,1965 年 2 月出生于四川苍溪,现为北京科技大学信息工程学院博士,已发表论文 20 余篇,感兴趣方向工业自动化控制及线性系统、非线性系统、混沌系统在保密通信中的应用研究.

郑德玲　女,1940 年 10 月出生于江西南昌,现为北京科技大学信息工程学院教授,博士生导师,已发表论文 100 余篇,现任中国自动化学会控制理论专业委员会委员,主要从事人工智能及应用,智能自动化技术及应用,神经及模糊控制,状态识别及混沌信息处理等方面的研究.