第 59 卷 第 5 期 2010 年 5 月
1000-3290/2010/59(05)/3017-10

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 5, May, 2010

基于数字信号处理器的语音无线混沌通信——系统设计与硬件实现*

张朝霞　禹思敏†

(广东工业大学自动化学院,广州　510006)

(2009 年 6 月 19 日收到;2009 年 9 月 21 日收到修改稿)

提出了一种基于数字信号处理器(DSP)的语音无线混沌数字通信系统设计与硬件实现的新方案. 根据 Runge-Kutta 算法和变量比例扩张变换,以多涡卷广义 Jerk 系统为例,对其连续混沌系统作离散化处理,产生作为语音数据加密与解密的混沌数字序列. 在芯片型号 TMS320VC5509APGE 的 DSP 技术平台上,利用无线发送器和无线接收器 nRF2401,实现了语音无线混沌数字通信. 给出了技术设计与硬件实现结果,证实了该方案的可行性.

关键词: 数字信号处理器,多涡卷广义 Jerk 系统,语音无线混沌数字通信,硬件实现
PACC: 0545

1. 引　　言

混沌在保密通信中应用是近年来直接为人类服务的重要研究方向之一,它的起源可追溯到 1990 年 Pecora 和 Carroll 提出混沌同步的概念[1]. 混沌保密通信经历了认识了解、深化研究到工程应用等多个不同阶段. 混沌信号以其类噪声式的宽带功率谱、冲击式的相关特性、对初始条件高度敏感性、复杂的混沌动力学行为,在混沌保密通信及其相关领域内获得了广泛应用[2—34]. 值得一提的是,目前,混沌通信已从理论分析、计算机仿真和电路实验阶段正逐步走入实际工程应用. 例如,文献[7]报道了利用光纤技术实现混沌保密通信的最新结果. 在技术实现方面,用数字信号处理器和现场可编程门阵列等先进的现代数字信号处理工具来实现混沌保密通信已成了一个实际可行的发展方向[10].

混沌通信分有线通信和无线通信两大类. 有线混沌通信因在理想信道中传输信号,混沌同步与混沌通信相对容易实现[17]. 但对于无线混沌通信来说,其实现的难度要比有线混沌通信大得多. 无线混沌通信又可分无线模拟通信和无线数字通信两种情况. 已有研究结果表明,对于无线模拟混沌通信,由于受到信道干扰和非线性失真的影响,加之模拟通信系统本身缺少相对应的信道纠错功能,混沌同步的实现相对要困难些,接收端解调的语音信号不理想[18]. 而对于无线混沌数字通信,由于通过信道传输的是二进制数字信号,与传输模拟信号相比,它具有较强的抗干扰能力,并且无线数字发送器和接收器本身还具有纠错功能,因而使得无线数字混沌通信具有更好的实际可行性.

最近,我们提出了一种用数字信号处理器(DSP)实现语音无线混沌数字通信的系统设计与硬件实验方案. 为便于 DSP 技术实现,首先必须对连续时间混沌系统作离散化处理和变量比例扩张变换. 离散化方法有简单 Euler 法、改进 Euler 法和 Runge-Kutta 法. 为保证离散化运算精度和稳定性,我们选用了 Runge-Kutta 法,并以多涡卷广义 Jerk 系统为例进行离散化处理. 在硬件实现方面,基于芯片型号为 TMS320VC5509APGE 的 DSP 开发平台,在发送端,通过 DSP 的离散迭代运算,实现混沌序列对语音数据的混沌加密,并将加密后的数据,通过无线发送和接收器 nRF2401,实现对加密数据的无线发送与接收. 在接收端,则根据自同步原理,

* 国家自然科学基金(批准号: 60572073, 60871025),广东省自然科学基金(批准号: 8151009001000060),广东省自然科学基金研究团队项目(批准号:8351009001000002)和广东省科技计划项目(批准号:2009B010800037)资助的课题.

† 通讯联系人. E-mail: siminyu@163.com

通过 DSP 实现对加密数据的混沌解密. 系统设计与硬件实现结果证实了该方案的有效性.

2. 对语音进行加密/解密时多涡卷广义 Jerk 系统同步原理与分析

混沌通信主要有相干通信和非相干通信两大类,而混沌同步是实现相干混沌通信的前提和基础. 为了在 DSP 硬件平台上实现相干混沌无线通信,首先应考虑以下三个主要问题:

1)在硬件实现的实际情况下,应选择适合于无线通信自同步的混沌系统. 当利用它们对语音信号进行加密、传输和解密时,应能保证发送端和接收端混沌系统较稳定的同步.

2)考虑到无线混沌通信对实时性的要求很高,并且在实际情况中往往系统受到硬件资源的制约,混沌加密和解密算法不能过于复杂,从而能保证无线混沌通信不会造成通信中断的现象,具有较好的实时性.

3)选用加密性能相对较好的混沌系统. 从混沌系统产生涡卷数量多少来分类,主要有双涡卷和多涡卷系统. 与双涡卷系统相比,多涡卷系统具有更多的涡卷密钥参数,即数量众多的涡卷能在相空间中呈现某个方向分布甚至多个方向分布的平面或立体网格状图案,涡卷之间具有相互嵌套的拓扑结构,涡卷的数量和网格状分布图案等可由系统的参数来控制,具有更为复杂的混沌动力学行为. 这种复杂性体现在混沌吸引子的相轨迹或状态变量的取值能在多个不同的涡卷之间随机地跳变,从而使得当涡卷的数量越多时,这种跳变的随机性就越大,更有利于语音信号的混沌加密.

基于上述三点考虑,可选用多涡卷广义 Jerk 系统来实现语音无线混沌数字通信. 下面分析这类混沌系统在实现语音信号加密和解密时的同步问题.

多涡卷广义 Jerk 系统[19]无量纲状态方程的数学表达式为

$$\begin{aligned}\dot{x} &= y,\\ \dot{y} &= z,\\ \dot{z} &= -\gamma y - \beta z + f(x),\end{aligned} \tag{1}$$

式中 $\beta = 0.6$, $\gamma = 1$, $f(x)$ 为锯齿波、三角波等多种不同类型的非线性函数. 不妨选取 $f(x)$ 为锯齿波的形式

$$\begin{aligned}f(x) &= \operatorname{sgn}(x) + \operatorname{sgn}(x-2) + \operatorname{sgn}(x+2)\\ &\quad + \operatorname{sgn}(x-4) + \operatorname{sgn}(x+4) - x.\end{aligned} \tag{2}$$

根据(1)式和(2)式,得 6 涡卷混沌吸引子的数值模拟结果如图 1 所示,该系统随参数 β 变化时最大李氏指数的计算结果如图 2 所示. 显见 6 涡卷广义 Jerk 系统的最大李氏指数为正,因而为混沌态.

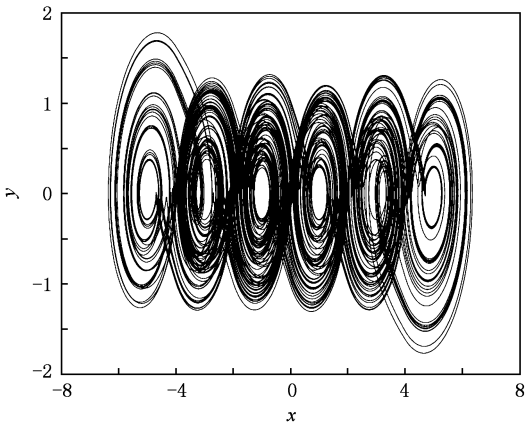

图 1 广义 Jerk 系统中的 6 涡卷混沌吸引子

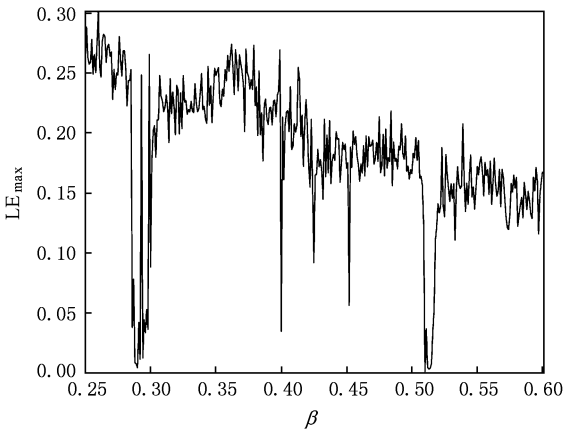

图 2 随参数 β 变化的最大李氏指数

注意到(1)式表示的多涡卷广义 Jerk 系统具有以下两个明显的特点:

1)$f(\cdot)$ 是方程中唯一的非线性项,并且仅只出现在第 3 个方程中.

2)状态变量 x 仅只出现在非线性函数 $f(\cdot)$ 中.

根据这两个特点,我们提出用非线性函数 $f(\cdot)$ 和状态变量 x 来实现对语音信号的加密和解密,并且证明(1)式表示的多涡卷广义 Jerk 系统用这种方法对语音信号进行加密和解密时,保证发送端与接收端混沌系统之间的同步.

设多涡卷广义 Jerk 系统发送端混沌系统的状

态变量为 $x^{(1)}, y^{(1)}, z^{(1)}$，得发送端混沌加密系统状态方程的数学表达式为

$$\begin{aligned}\dot{x}^{(1)} &= y^{(1)},\\ \dot{y}^{(1)} &= z^{(1)},\\ \dot{z}^{(1)} &= -\gamma y^{(1)} - \beta z^{(1)} + f(p),\end{aligned} \tag{3}$$

式中 $p(t)$ 为加密器 $E(t)$ 输出信号. 注意到(3)式和(1)式的不同之处在于用 $p(t)$ 取代了非线性函数 $f(\cdot)$ 中的自变量 x. 而 $p(t)$ 则是利用非线性函数 $f(\cdot)$ 和状态变量 $x^{(1)}$ 来实现对输入语音信号 $s(t)$ 进行加密后的信号，其数学表达为

$$p(t) = x^{(1)}(t) \oplus \{\mathrm{H}[s(t)]\}, \tag{4}$$

式中⊕表示某种具体的加密运算，而 H 则表示对语音信号本身进行的某种处理或置乱运算. 由于混沌无线通信对实时性的要求很高，加密和解密算法不能过于复杂，这样才能保证混沌无线通信具有较好的实时性. 此外，为保证对语音信号进行加密和解密时，混沌系统本身能保持较好的稳定性，应满足 $|x^{(1)}(t)/\{\mathrm{H}[s(t)]\}|_{\max} \geqslant 10^2$.

设多涡卷广义 Jerk 系统接收端混沌系统的状态变量为 $x^{(2)}, y^{(2)}, z^{(2)}$，并将混沌加密后的信号 $p(t)$ 经信道传输至接收端，得接收端混沌解密系统状态方程的数学表达式为

$$\begin{aligned}\dot{x}^{(2)} &= y^{(2)},\\ \dot{y}^{(2)} &= z^{(2)},\\ \dot{z}^{(2)} &= -\gamma y^{(2)} - \beta z^{(2)} + f(p).\end{aligned} \tag{5}$$

在接收端，对接收到的加密信号进行解密，解密器 $D(t)$ 的输出为

$$\hat{s}(t) = \mathrm{H}^{-1}[x^{(2)}(t) \otimes p(t)], \tag{6}$$

式中 $\hat{s}(t)$ 为解密器 $D(t)$ 输出的语音信号，$x^{(2)}(t)$ 为接收端混沌信号，⊗表示与⊕对应的逆运算，H^{-1} 表示与 H 对应的逆运算. 解密器 $D(t)$ 能否正确解密，分以下三种情况：

1)接收端混沌系统参数与发送端不严格匹配或加密后的信号 $p(t)$ 通过信道传输受到干扰和非线性失真而不能实现同步时，$x^{(2)} \neq x^{(1)}$. 根据(6)式，得 $\hat{s}(t) \neq s(t)$，接收端混沌系统无法正确解密出原语音信号.

2)接收端与发送端混沌系统实现同步时，$x^{(2)} = x^{(1)}$. 根据(6)式，得 $\hat{s}(t) = s(t)$，能正确解密出原语音信号.

3)接收端混沌系统与发送端混沌系统能实现同步，但存在一个恒定的同步误差 C_1，即 $x^{(2)} = x^{(1)} - C_1$，其中 C_1 为常量. 由(6)式，得 $\hat{s}(t) = s(t) - C_1$，这表明仅在原语音信号上叠加了一个直流分量 C_1，并不影响对原语音信号的正确解密.

下面证明(3)式和(5)式对语音信号加密和解密时的同步能满足上述第三种情况. 设状态变量误差信号分别为 $e_x = x^{(1)} - x^{(2)}$，$e_y = y^{(1)} - y^{(2)}$，$e_z = z^{(1)} - z^{(2)}$，经分析和推导，可得关于(3)式和(5)式误差信号的微分方程为

$$\dddot{e}_x + \beta \ddot{e}_x + \gamma \dot{e}_x = 0. \tag{7}$$

注意到(7)式的特征方程为 $\lambda^3 + \beta\lambda^2 + \gamma\lambda = 0$，对应的三个特征值分别为 $\lambda_0 = 0$，$\lambda_{1,2} = -\alpha \pm \mathrm{j}\omega$，其中 $\alpha = \beta/2$，$\omega = \sqrt{\gamma - \alpha^2}$. 已知 $\beta = 0.6$，$\gamma = 1$，进一步得 $\alpha = \beta/2 = 0.3$，$\omega = \sqrt{\gamma - \alpha^2} = 0.9539$. 最后可得关于误差信号微分方程(7)式的通解为

$$\begin{aligned}e_x &= C_1 \mathrm{e}^{-\lambda_0 t} + C_2 \mathrm{e}^{-\lambda_1 t} + C_3 \mathrm{e}^{-\lambda_2 t}\\ &= C_1 + \mathrm{e}^{-\alpha t}[A_1 \cos\omega t + B_1 \sin\omega t],\\ e_y &= D_1 \mathrm{e}^{-\lambda_1 t} + D_2 \mathrm{e}^{-\lambda_2 t}\\ &= \mathrm{e}^{-\alpha t}[A_2 \cos\omega t + B_2 \sin\omega t],\\ e_z &= E_1 \mathrm{e}^{-\lambda_1 t} + E_2 \mathrm{e}^{-\lambda_2 t}\\ &= \mathrm{e}^{-\alpha t}[A_3 \cos\omega t + B_3 \sin\omega t],\end{aligned} \tag{8}$$

式中 $A_i, B_i (i = 1,2,3)$，$C_i (i = 1,2,3)$，$D_i (i = 1,2)$，$E_i (i = 1,2)$ 均为常数，其大小只与系统的初始值有关. 若设误差的初始值为 $e_x(0)$，$e_y(0)$，$e_z(0)$，根据(8)式，得

$$\begin{aligned}e_x(0) &= A_1 + C_1,\\ \dot{e}_x(0) &= -\alpha A_1 + \omega B_1 = e_y(0),\\ \ddot{e}_x(0) &= (\alpha^2 - \omega^2) A_1 - 2\alpha\omega B_1 = e_z(0),\\ e_y(0) &= A_2,\\ \dot{e}_y(0) &= -\alpha A_2 + \omega B_2 = e_z(0),\\ e_z(0) &= A_3,\\ \dot{e}_z(0) &= -\alpha A_3 + \omega B_3 = -\gamma e_y(0) - \beta e_z(0).\end{aligned} \tag{9}$$

由(9)式，进一步得

$$\begin{aligned}A_1 &= -\frac{2\alpha e_y(0) + e_z(0)}{\omega^2 + \alpha^2},\\ B_1 &= \frac{e_y(0) + \alpha A_1}{\omega^2 + \alpha^2},\\ C_1 &= e_x(0) - A_1,\\ A_2 &= e_y(0),\\ B_2 &= \frac{e_z(0) + \alpha e_y(0)}{\omega},\\ A_3 &= e_z(0),\\ B_3 &= \frac{-\gamma e_y(0) + (\alpha - \beta) e_z(0)}{\omega}.\end{aligned} \tag{10}$$

根据(10)式,得(8)式中的各个 A_i,B_i($i=1,2,3$)和 C_1 均为常数,其大小只与系统的初始值$e_x(0)$,$e_y(0)$,$e_z(0)$有关,一旦 $e_x(0)$,$e_y(0)$,$e_z(0)$给定,A_i,B_i($i=1,2,3$)和 C_1 也随之确定,并且是不变的常量.

由此可得出如下结论:同步误差,e_x,e_y, e_z 均按指数规律 $e^{-\alpha t}$收敛, 从而有 $e_x\to C_1$,$e_x\to 0$,$e_z\to 0$. 到达同步后,$x^{(2)}=x^{(1)}-C_1$,$y^{(2)}=y^{(1)}$,$z^{(2)}=z^{(1)}$.

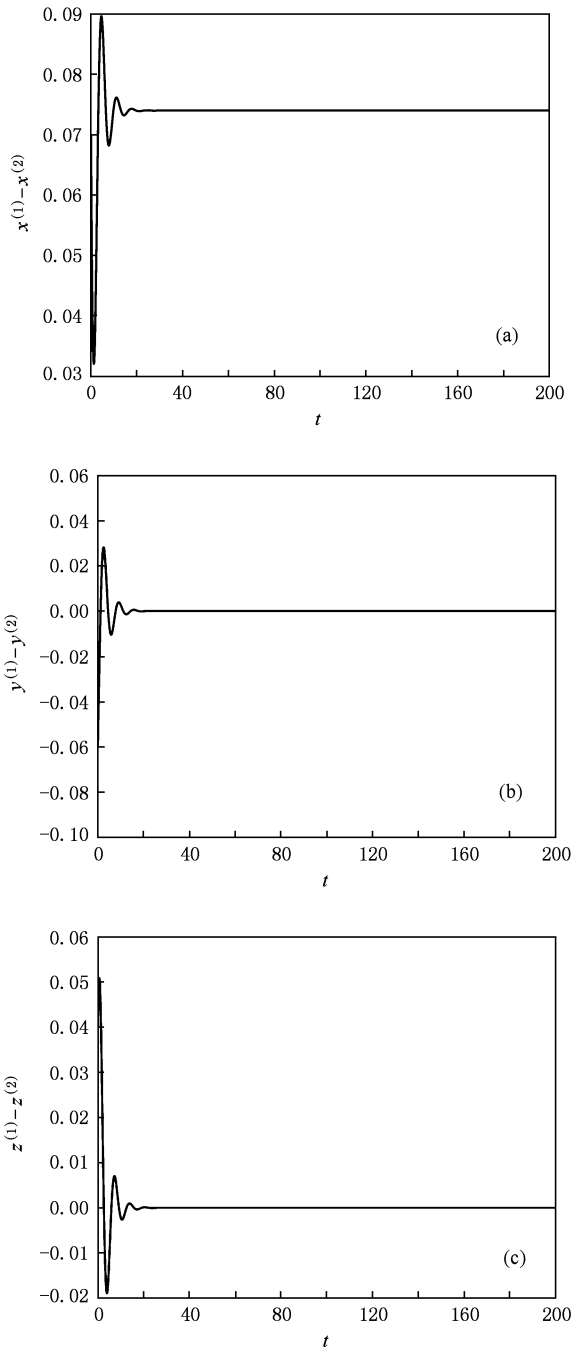

图3 6涡卷广义 Jerk 系统同步误差的数值模拟结果 (a)误差信号 e_x; (b)误差信号 e_y; (c)误差信号 e_z

设发送端混沌系统的初始值分别为 $x^{(1)}(0)=0.02$,$y^{(1)}(0)=0.01$,$z^{(1)}(0)=0.12$,接收端混沌系统的初始值为 $x^{(2)}(0)=-0.05$,$y^{(2)}(0)=0.07$,$z^{(2)}(0)=0.08$. 得误差信号为 $e_x(0)=0.07$, $e_y(0)=-0.06$, $e_z(0)=0.04$. 根据(8)式,得 $x^{(2)}$ 与 $x^{(1)}$ 之间的固定误差为 $C_1=0.074$,显见 C_1 为常量. 发送端与接收端系统同步误差的数值模拟结果如图3所示.

3. 用 Runge-Kutta 算法实现多涡卷广义 Jerk 系统的离散化

为了能在 DSP5509 技术平台上实现混沌数字无线通信,首先必须对多涡卷广义 Jerk 系统作离散化处理,我们采用了精度较高和稳定性较好的 Runge-Kutta 算法来实现连续时间混沌系统的离散化. 此外,为保证混沌系统受到语音信号的调制时的稳定性,要求混沌信号比语音信号大两个数量级以上,即满足 $|x^{(1)}(t)/\{H[s(t)]\}|_{\max}\geqslant 10^2$,故还需要对混沌系统作变量比例扩张变换.

根据(3)式和 Runge-Kutta 算法,得发送端多涡卷广义 Jerk 系统的离散化方程为

$$\begin{aligned}x^{(1)}(n+1)&=x^{(1)}(n)+(K_{11}^{(1)}+2K_{12}^{(1)}\\&\quad+2K_{13}^{(1)}+K_{14}^{(1)})/6,\\y^{(1)}(n+1)&=y^{(1)}(n)+(K_{21}^{(1)}+2K_{22}^{(1)}\\&\quad+2K_{23}^{(1)}+K_{24}^{(1)})/6,\\z^{(1)}(n+1)&=z^{(1)}(n)+(K_{31}^{(1)}+2K_{32}^{(1)}\\&\quad+2K_{33}^{(1)}+K_{34}^{(1)})/6,\end{aligned}\tag{11}$$

式中 $K_{11}^{(1)}$,$K_{21}^{(1)}$,$K_{31}^{(1)}$ 计算公式的数学表达式为

$$\begin{aligned}K_{11}^{(1)}&=T\cdot y^{(1)}(n),\\K_{21}^{(1)}&=T\cdot z^{(1)}(n),\\K_{31}^{(1)}&=T\cdot[-\gamma y^{(1)}(n)-\beta z^{(1)}(n)+f^{(1)}(p(n))],\end{aligned}\tag{12}$$

其中 $p(n)=x^{(1)}(n)\oplus\{\mathrm{H}[s(n)]\}$ 为发送端加密器 $E(n)$输出混沌加密后的数据,$s(n)$为离散化后的语音数据,$\oplus$为加法运算,H 表示对 $s(n)$的位置乱运算. 同理,得 $K_{12}^{(1)}$,$K_{22}^{(1)}$,$K_{32}^{(1)}$和 $K_{13}^{(1)}$,$K_{23}^{(1)}$,$K_{33}^{(1)}$计算公式的数学表达式为

$$\begin{aligned}K_{1j}^{(1)}&=T\cdot[y^{(1)}(n)+0.5K_{2,j-1}^{(1)}],\\K_{2j}^{(1)}&=T\cdot[z^{(1)}(n)+0.5K_{3,j-1}^{(1)}],\end{aligned}$$

$$K_{3j}^{(1)} = T\cdot[-\gamma(y^{(1)}(n)+0.5K_{2,j-1}^{(1)})-\beta(z^{(1)}(n)+0.5K_{3,j-1}^{(1)})+f^{(1)}(p(n)+0.5K_{1,j-1}^{(1)})]. \quad (13)$$

式中 $j=2,3$. 同理,得 $K_{14}^{(1)}$,$K_{24}^{(1)}$,$K_{34}^{(1)}$ 计算公式的数学表达式为

$$K_{14}^{(1)} = T\cdot[y^{(1)}(n)+K_{23}^{(1)}],$$
$$K_{24}^{(1)} = T\cdot[z^{(1)}(n)+K_{33}^{(1)}],$$
$$K_{34}^{(1)} = T\cdot[-\gamma(y^{(1)}(n)+K_{23}^{(1)})-\beta(z^{(1)}(n)+K_{33}^{(1)})+f^{(1)}(p(n)+K_{13}^{(1)})]. \quad (14)$$

上面各式中的参数为 $\beta=0.6$,$\gamma=1$,$T=0.1$ 为满足取样定理的取样时间,$A=500$ 为变量比例扩张系数. 此外,注意到上面各式中 $f^{(1)}(u)$ 数学表达式的一般形式为

$$f^{(1)}(u) = A[\mathrm{sgn}(u)+\mathrm{sgn}(u-2A)+\mathrm{sgn}(u-4A)+\mathrm{sgn}(u+2A)+\mathrm{sgn}(u+4A)]-u, \quad (15)$$

其中 u 为各个式子相对应的复合变量.

将发送端混沌加密后的数据 $p(n)=x^{(1)}(n)\oplus\{\mathrm{H}[s(n)]\}$ 经信道传输至接收端,根据(5)式和 Runge-Kutta 算法,得接收端多涡卷广义 Jerk 系统的离散化方程为

$$x^{(2)}(n+1) = x^{(2)}(n)+(K_{11}^{(2)}+2K_{12}^{(2)}+2K_{13}^{(2)}+K_{14}^{(2)})/6,$$
$$y^{(2)}(n+1) = y^{(2)}(n)+(K_{21}^{(2)}+2K_{22}^{(2)}+2K_{23}^{(2)}+K_{24}^{(2)})/6,$$
$$z^{(2)}(n+1) = z^{(2)}(n)+(K_{31}^{(2)}+2K_{32}^{(2)}+2K_{33}^{(2)}+K_{34}^{(2)})/6. \quad (16)$$

式中 $K_{11}^{(2)}$,$K_{21}^{(2)}$,$K_{31}^{(2)}$ 计算公式的数学表达式为

$$K_{11}^{(2)} = T\cdot y^{(2)}(n),$$
$$K_{21}^{(2)} = T\cdot z^{(2)}(n),$$
$$K_{31}^{(2)} = T\cdot[-\gamma y^{(2)}(n)-\beta z^{(2)}(n)+f^{(2)}(p(n))], \quad (17)$$

同理,得 $K_{12}^{(2)}$,$K_{22}^{(2)}$,$K_{32}^{(2)}$ 和 $K_{13}^{(2)}$,$K_{23}^{(2)}$,$K_{33}^{(2)}$ 计算公式的数学表达式为

$$K_{1j}^{(2)} = T\cdot[y^{(2)}(n)+0.5K_{2,j-1}^{(2)}],$$
$$K_{2j}^{(2)} = T\cdot[z^{(2)}(n)+0.5K_{3,j-1}^{(2)}],$$
$$K_{3j}^{(2)} = T\cdot[-\gamma(y^{(2)}(n)+0.5K_{2,j-1}^{(2)})-\beta(z^{(2)}(n)+0.5K_{3,j-1}^{(2)})+f^{(2)}(p(n)+0.5K_{1,j-1}^{(2)})], \quad (18)$$

式中 $j=2,3$. 同理,得 $K_{14}^{(2)}$,$K_{24}^{(2)}$,$K_{34}^{(2)}$ 计算公式的数学表达式为

$$K_{14}^{(2)} = T\cdot[y^{(2)}(n)+K_{23}^{(2)}],$$
$$K_{24}^{(2)} = T\cdot[z^{(2)}(n)+K_{33}^{(2)}],$$
$$K_{34}^{(2)} = T\cdot[-\gamma(y^{(2)}(n)+K_{23}^{(2)})-\beta(z^{(2)}(n)+K_{33}^{(2)})+f^{(2)}(p(n)+K_{13}^{(2)})]. \quad (19)$$

上面各式中的参数为 $\beta=0.6$,$\gamma=1$,$T=0.1$ 为满足取样定理的取样时间,$A=500$ 为变量比例扩张系数. 此外,注意到上面各式中 $f^{(2)}(v)$ 数学表达式的一般形式为

$$f^{(2)}(v) = A[\mathrm{sgn}(v)+\mathrm{sgn}(v-2A)+\mathrm{sgn}(v-4A)+\mathrm{sgn}(v+2A)+\mathrm{sgn}(v+4A)]-v, \quad (20)$$

其中 v 为各个式子相对应的复合变量.

在接收端,对接收到的加密信号进行解密,解密器 $D(n)$ 的输出为

$$\hat{s}(n) = \mathrm{H}^{-1}[x^{(2)}(n)\otimes p(n)], \quad (21)$$

式中 $\hat{s}(n)$ 为解密器 $D(n)$ 输出的语音信号,$x^{(2)}(n)$ 为接收端混沌信号,$\otimes$ 表示与 $\oplus$ 对应的逆运算,即减法运算,H^{-1} 表示与 H 相对应的反置乱运算.

4. 语音无线混沌数字通信系统的硬件与软件设计

在对语音信号加密与解密时多涡卷广义 Jerk 系统同步原理的分析以及用 Runge-Kutta 算法对其作离散化处理和变量比例扩张变换的基础上,本节进一步对语音无线混沌数字通信系统的硬件与软件进行设计.

4.1. 语音无线混沌数字通信系统的硬件设计

DSP 是一种用于实时、快速实现各种数字信号处理算法的器件. 在本实验系统中,我们采用了语音数字通信与信号处理的两款较高档产品 TMS320VC5509APGE 来实现语音无线混沌数字通信,其中一款用于语音信号的混沌加密,另一款用于语音信号的混沌解密. 数字无线发送器和接收器则采用了两款相同的模块 nRF2401,其传输比特率为 1 MHz/s,能满足传送语音信号的要求,并具有纠错功能. 其中一款用于数字无线发送,另一款用于数字无线接收. 语音无线混沌数字通信硬件实验系统如图 4 所示,相对应的语音无线混沌数字通信硬件实验系统的原理设计框图如图 5 所示.

在图 4 和图 5 中,涉及到与硬件实现相关的主要部件、功能及连接关系如下:

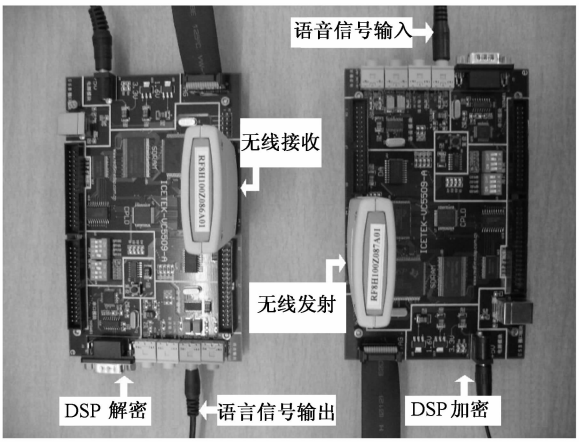

图 4 语音无线混沌数字通信硬件实验系统

1)TMS320VC5509APGE 片上的主要资源:主频为 200 MHz,处理性能为 400MIPS,双核. RAM 为 128 k×16 bit,ROM 为 32 k×16 bit.

2)初始化配置:DSP 通过 I^2C 总线将配置命令发送到 A/D 和 D/A 转换器 AIC23,配置完成后,AIC23 开始工作.

3)语音信号的输入:AIC23 通过其中的 A/D 转换器采集输入的语音信号,等采集完一个数据后,将数据发送到 DSP 的多通道缓冲串口 MCBCP0 接口上,DSP 可以读取到语音数据,每个数据为 16 位无符号整数.

4)语音信号的输出:DSP 可以将语音数据通过 MCBSP0 接口发送给 AIC23,AIC23 的 D/A 转换器

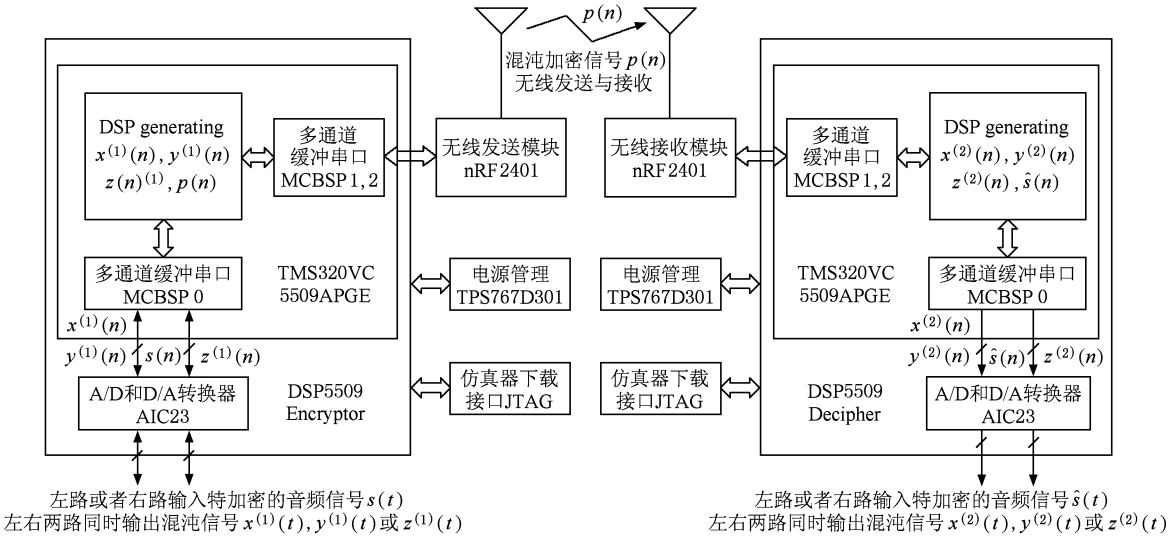

图 5 语音无线混沌数字通信硬件实验系统的原理设计框图

将其转换成模拟信号输出.

5)无线发送和接收器 nRF2401 工作模式:它们均工作在 ShockBurstTM 收发模式,该模式使用了片内的先入先出堆栈区 FIFO,数据低速从 DSP 送入,高速(1Mbps)发射,与射频协议相关的所有高速信号处理均在 nRF2401 片内进行. 无线发送器 nRF2401 首先将来自发送端 MCBSP1 的语音加密数据自动加上字头和 CRC 校验码,再由射频发送出去. 无线接收器 nRF2401 在接收到来自无线发送器 nRF2401 的数据时,自动把字头和 CRC 校验码移去,当接收完数据后,通过把引脚 DR1 置成低电平,从而触发 TMS320VC5509A 的外部中断 INT2,TMS320VC5509A 立即响应中断 INT2,开始从无线接收器 nRF2401 读取语音加密数据并存入先入先出堆栈区 FIFO 中.

6)MCBSP0 与 AIC23、发送端 MCBSP1,2 与无线发送器、接收端 MCBSP1,2 与无线接收器 nRF2401 的硬件连接图如图 6 所示.

4.2. 语音无线混沌数字通信系统的软件设计

在用 Runge-Kutta 算法对多涡卷广义 Jerk 系统作离散化处理和变量比例扩张变换的基础上,根据图 4—6 所示的硬件设计与实现平台,需要对其软件系统进行相应的设计. 其中发送端主程序流程图如图 7 所示,接收端主程序流程图如图 8 所示.

当无线接收器 NRF2401 接收到完整的数据包

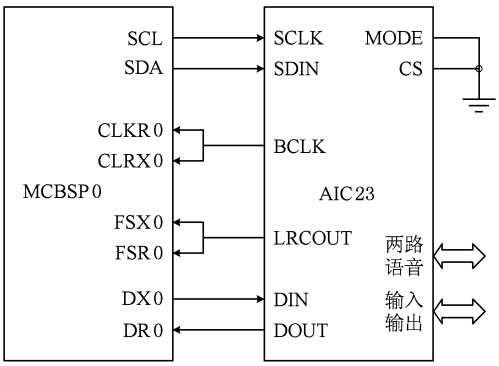

图 6　硬件连接图　（a）MCBSP0 与 AIC23 连接图；（b）MCBSP1,2 与无线发送器连接图；（c）MCBSP1,2 与无线接收器连接图

后，通过置引脚 DR1 为低电平，从而触发 TMS320VC5509APGE 外部中断 2，并通过调用接收端中断服务程序实时响应该中断. 接收端中断服务程序的流程图如图 9 所示.

4.3. 硬件与软件设计方案的实现

根据图 4—9 所示的硬件和软件设计方案，对其主要实现过程归纳如下：

1）利用图 5 中的立体声音频编码/解码（Codec）芯片 TLV320AIC23B 将输入的语音信号 $s(t)$ 转换成离散信号 $s(n)$.

2）在发送端，首先任意给定一组不全为 0 的初始值 $x^{(1)}(0), y^{(1)}(0), z^{(1)}(0)$. DSP 然后根据迭代

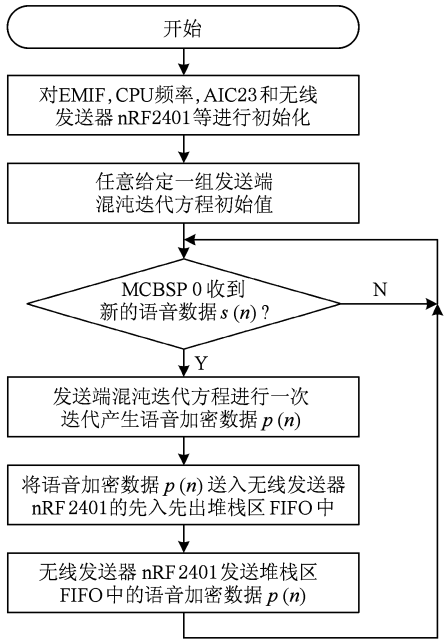

图 7　发送端主程序流程图

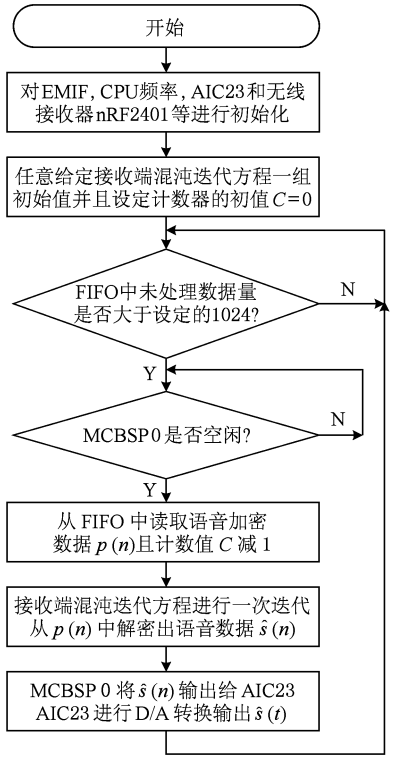

图 8　接收端主程序流程图

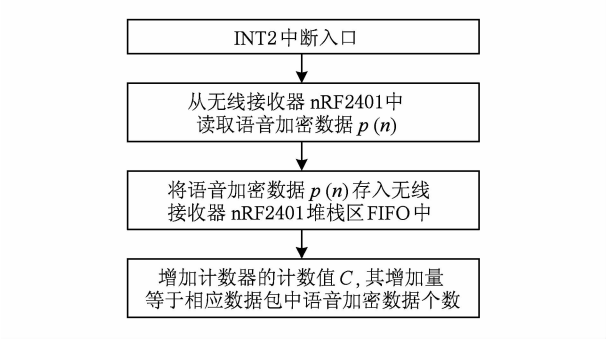

图 9 接收端中断服务程序流程图

方程(11)—(15)式以及输入语音数据 $s(n)$ 作循环迭代运算,进而产生迭代序列 $x^{(1)}(n)$, $y^{(1)}(n)$, $z^{(1)}(n)$ 和加密数据 $p(n)$ ($n=0,1,2,3,\cdots$),其软件实现流程如图 7 所示.

3)混沌加密后的数据 $p(n)$ 通过数字无线发送器 nRF2401 发送至接收端.

4)在接收端,先任给一组不全为 0 初始值 $x^{(2)}(0)$, $y^{(2)}(0)$, $z^{(2)}(0)$. 收到 $p(n)$ 后,DSP 根据迭代方程(16)—(21)以及接收到的加密数据 $p(n)$ 作循环迭代运算,进而产生迭代序列 $x^{(2)}(n)$, $y^{(2)}(n)$, $z^{(2)}(n)$, $\hat{s}(n)$,最后解密出语音数据 $\hat{s}(n)$,其软件实现流程如图 8 所示.

5)接收端的数字无线接收器 nRF2401 与 DSP 相互配合,通过外部中断 INT2 的中断方式接收加密数据 $p(n)$,其软件实现流程如图 9 所示.

6)接收端对迭代序列 $x^{(2)}(n)$, $y^{(2)}(n)$, $z^{(2)}(n)$ 进行变量比例压缩变换. 变量比例压缩变换因子为 $1/A$,经压缩变换后恢复成序列 $x(n)$, $y(n)$, $z(n)$.

7)利用图 5 中立体声音频编码/解码芯片 TLV320AIC23B 将 $x(n)$, $y(n)$, $z(n)$, $\hat{s}(n)$ 中的两路转换成模拟信号,送到示波器上显示. 例如,若将 $x(n)$, $y(n)$, $z(n)$ 转换成模拟信号,可从示波器上观察到混沌吸引子的相图. 若将 $\hat{s}(n)$ 转换成模拟信号 $\hat{s}(t)$,可从示波器上同时观察输入端语音信号 $s(t)$ 和接收端解调出语音信号 $\hat{s}(t)$ 的时域波形,从而进行对比和分析.

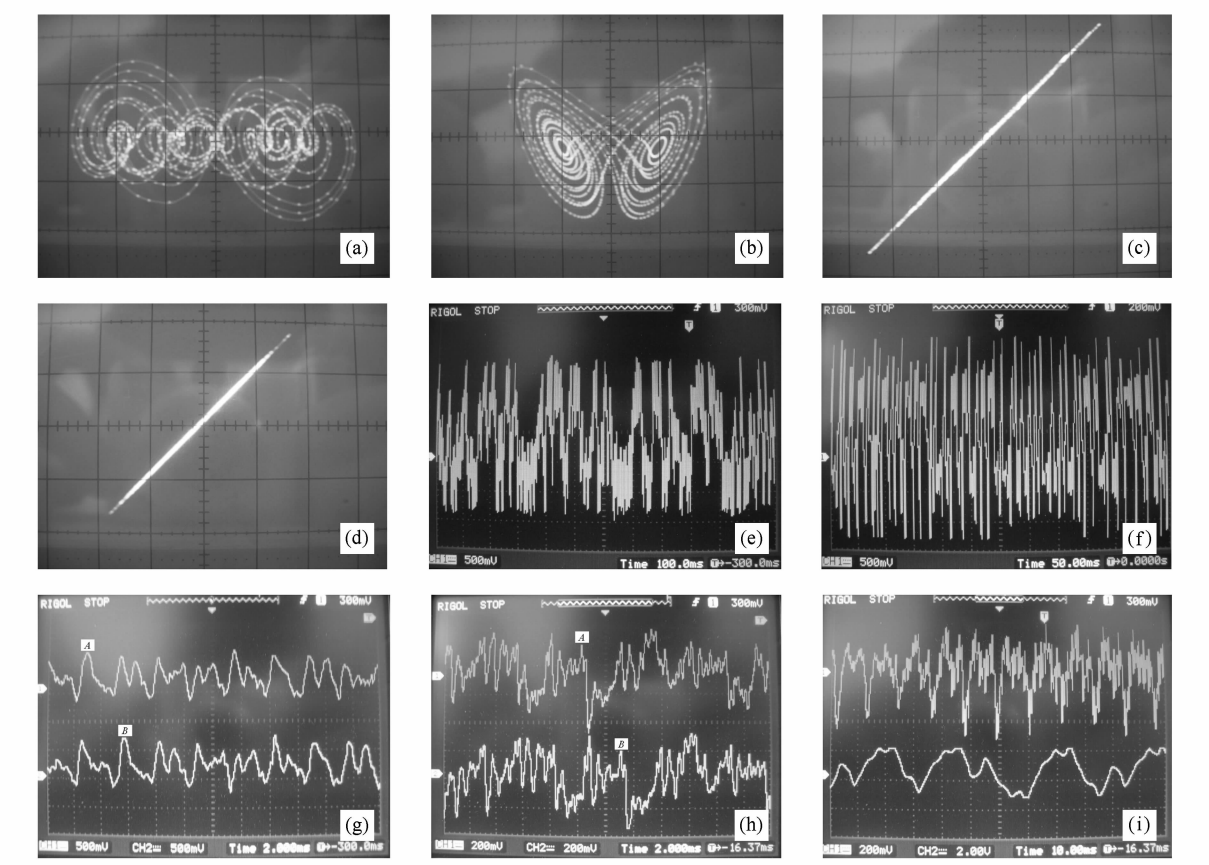

图 10 语音无线混沌数字通信的硬件实验结果 (a)经 $s(n)$ 调制后的 6 涡卷 Jerk 吸引子;(b)经 $s(n)$ 调制后的 Lorenz 吸引子;(c)发送端与接收端 Jerk 系统同步相图;(d)发送端与接收端 Lorenz 系统同步相图;(e)Jerk 系统无线发送加密信号 $p(n)$;(f)Lorenz 系统无线发送加密信号 $p(n)$;(g)Jerk 系统正确解调出的语音信号;(h)Lorenz 系统正确解调出的语音信号;(i)参数失配的语音信号解调结果

5. 语音无线混沌数字通信的硬件实现结果

根据上述硬件和软件设计方案，进行语音无线混沌数字通信的硬件实验，实现结果如图 10 所示. 需要强调的是，这种硬件和软件实现方案对某些混沌系统来说，具有一定的普适性. 例如，在图 10 中，我们还进一步给出了用 Lorenz 系统的驱动-响应式同步来实现语音混沌加密和解密结果. 有关图 10 所示硬件实验结果的两点说明如下：

1）由于 DSP 芯片 TMS320VC5509APGE 为 32 位浮点运算，具有很高的运算精度，从而保证了当接收端混沌系统与发送端混沌系统之间的参数匹配时，恢复出的语音信号具有较高的保真度，如图 10(g)和(h)所示，其中上图为发送端输入的语音信号，下图为接收端解密出的语音信号，两者除存在一定的延时以外（如图中的 A，B 对应点），可看出还原出语音信号的保真度较好.

2）对于混沌通信的数值仿真，由于不涉及到硬件实现及实时性等问题，是一种理想的情况，为提高加密算法的安全性能，混沌加密方案一般都较为复杂. 但在硬件实现的实际情况下，考虑到无线混沌通信对实时性的要求很高，并且在实际情况中往往受到系统硬件资源的制约，为保证无线混沌通信不造成通信中断现象，有较好的实时性，因而混沌加密和解密算法不能过于复杂. 这里采用了混沌加密与传统加密（即前面提及的语音数据置乱）方案相结合的方法来改善安全性能. 当接收端与发送端之间的任何一个参数有很小的失配时，便无法正确解调出原语音信号，图 10(i)示出了当参数 β 失配为 1% 时的硬件实验结果. 从这个角度来讲，混沌通信的安全性主要体现在对参数匹配的高度敏感性，当窃听一方在事先不知道原系统参数的情况下，要想破译有用信息有较大的难度.

6. 结　　论

混沌通信分有线通信和无线通信两大类. 有线混沌通信因在理想信道中传输信号，混沌同步与通信相对容易实现. 但对于无线混沌通信来说，其实现的难度要比有线混沌通信大得多. 我们设计了无线混沌数字通信的硬件与软件系统，并以多涡卷广义 Jerk 系统为例，用 Runge-Kutta 算法作离散化处理，利用 DSP 技术平台以及无线发送和接收器 nRF2401，成功地实现了语音无线混沌数字通信. 与无线混沌模拟通信相比，无线混沌数字通信由于在信道中传输的是二进制数字信号，具有较强的抗干扰能力，并且数字无线发送和接收器本身所具有的纠错功能，使得无线混沌数字通信具有更好的实际可行性，这一结论已被硬件实现结果所证实.

[1] Pecora L M, Carroll T L 1990 *Phys. Review Lett.* **64** 821

[2] Yang T, Chua L O 1996 *IEEE Trans. CAS-I* **43** 817

[3] Dedieu H, Kennedy M P 1993 *IEEE Trans. CAS-I* **40** 634

[4] Yang T, Chua L O 1997 *Int. J. Bifurc. Chaos* **7** 2789

[5] Feldmann U, Hasler M, Schwarz W 1996 *Int. J. Circuit Theory Appl.* **24** 551

[6] Halle K S, Wu C W, Itoh M, Chua L O 1993 *Int. J. Bifurc. Chaos* **3** 469

[7] Apostolos A 2005 *Nature* **437** 343

[8] Sushchik M, Rulkov N, larson L, tsimring L, Abarbanel H, Yao K 2000 *IEEE Commun. Lett.* **4** 128

[9] Khadra A, Liu X Z, Shen X 2005 *Automatica* **41** 1491

[10] Cong L, Xiaofu W 2001 *IEEE Trans. CAS-I* **48** 521

[11] Lü J H, Chen G R 2006 *Int. J. Bifurc. Chaos* **16** 775

[12] Suykens J A K, Vandewalle J 1993 *IEEE Trans. CAS-I* **40** 861

[13] Yalcin M E, J. Suykens J A K, Vandewalle J, Ozoguz S 2002 *Int. J. Bifurc. Chaos* **12** 23

[14] Lü J H, Yu S M, Leung H, Chen G R 2006 *IEEE Trans. CAS-I* **53** 149

[15] Yu S M, Lü J H, Chen G R 2007 *IEEE Trans. CAS – I* **54** 2087

[16] Milanovic V, Zaghloul M E 1996 *Electron. Lett.* **32** 11

[17] Zhou W J, Yu S M 2009 *Acta Phys. Sin.* **58** 113 (in Chinese) [周武杰、禹思敏 2009 物理学报 **58** 113]

[18] Dmitriev A S, Panas A I, Starkov S O 1997 *Int. J. Bifurc. Chaos* **7** 2511

[19] Yu S M, Lü J H, Leung H, Chen G R 2005 *IEEE Trans. Circuits Syst.* Ⅰ **52** 1459

[20] Chen L, Wang D S 2007 *Acta Phys. Sin.* **56** 5661(in Chinese) [谌　龙、王德石 2007 物理学报 **56** 5661]

[21] Li Y X 2008 *J Commu.* **29** 46(in Chinese) [李育贤 2008 通信学报 **29** 46]

[22] Yan S L 2005 *Acta Electro. Sin.* **33** 267 (in Chinese) [颜森林 2005 电子学报 **33** 267]

[23] Liu F C, Liang X M, Song J Q 2008 *Acta Phys. Sin.* **57** 1458

(in Chinese) [刘福才、梁晓明、宋佳秋 2008 物理学报 **57** 1458]
[24] Yu N, Ding Q, Chen H 2007 *J. Commu.* **28** 73 (in Chinese) [于 娜、丁 群、陈 红 2007 通信学报 **28** 73]
[25] Yu S M, Qiu S S 2002 *J. Commu.* **23** 105 (in Chinese) [禹思敏、丘水生 2002 通信学报 **23** 105]
[26] Zhang Y, Chen T Q, chen B 2007 *Acta Phys. Sin.* **56** 56 (in Chinese) [张 勇、陈天麒、陈 滨 2007 物理学报 **56** 56]
[27] Yan S L, Wang S Q 2006 *Acta Phys. Sin.* **55** 1687 (in Chinese) [颜森林、汪胜前 2006 物理学报 **55** 1687]
[28] Sun L, Jiang D P 2006 *Acta Phys. Sin.* **55** 3283 (in Chinese) [孙 琳、姜德平 2006 物理学报 **55** 3283]
[29] Zhang P S, Zhu Y S 2007 *J. Electro. Infor. Techn.* **29** 2359 (in Chinese) [赵柏山、朱义胜 2007 电子与信息学报 **29** 699]
[30] He H J, Zhang J S 2006 *J. Commu.* **27** 80 (in Chinese) [和红杰、张家树 2006 通信学报 **27** 80]
[31] Sun K H, Zhou J L, Mou J 2007 *J. Electro. Infor. Techn.* **29** 2436 (in Chinese) [孙克辉、周家令、牟 俊 2007 电子与信息学报 **29** 2436]
[32] Wang F P, Wang Z J, Guo J B 2003 *Acta Electro. Sin.* **31** 127 (in Chinese) [汪芙平、王赞基、郭静波 2003 电子学报 **31** 127]
[33] Han J Q, Zhu Y S 2006 *J. Electro. Infor. Techn.* **28** 2359 (in Chinese) [韩建群、朱义胜 2006 电子与信息学报 **28** 2359]
[34] Liao N H, Gao J F 2006 *J. Electro. Infor. Techn.* **28** 1255 (in Chinese) [廖旎焕、高金峰 2006 电子与信息学报 **28** 1255]

Wireless chaotic speech communication via digital signal processor ——system design and hardware implementation*

Zhang Chao-Xia Yu Si-Min†

(*College of Automation, Guangdong University of Technology, Guangzhou* 510006, *China*)

(Received 19 June 2009; revised manuscript received 21 September 2009)

Abstract

In this paper, a novel approach for system design and hardware realization of wireless chaotic digital speech communication via digital signal processor (DSP) is proposed. According to Runge-Kutta algorithm and variable ratio expansion transformation, taking multi-scroll generalized Jerk as an example, the continuous chaotic system is converted to the discrete chaotic one so as to generate chaotic digital sequences, which are used for speech data encryption and decryption. Based on the DSP technical platform with TMS320VC5509APGE chip, by utilizing nRF2401 wireless transmitter and receiver, wireless chaotic digital speech communication is successfully implemented. The results of technical design and hardware realization are also given, which confirms the feasibility of the scheme.

Keywords: digital signal processor, multi-scroll generalized Jerk system, wireless chaotic digital speech communication, hardware implementation

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60572073, 60871025), the Natural Science Foundation of Guangdong Province (Grant No. 8151009001000060), the Natural Science Foundation of Guangdong Province on Innovation Research Group (Grant No. 8351009001000002) and the Science and Technology Plan Project of Guangdong Province (Grant No. 2009B010800037).

† Corresponding author. E-mail: siminyu@163.com