第 56 卷 第 1 期 2007 年 1 月
1000-3290/2007/56(01)/0056-11

物 理 学 报
ACTA PHYSICA SINICA

Vol.56, No.1, January, 2007

跃变参数混沌同步及其应用

张 勇[1)2)] 陈天麒[1)] 陈 滨[1)]

1)(电子科技大学电子工程学院,成都 610054)

2)(江西财经大学,南昌 330013)

(2006 年 3 月 14 日收到;2006 年 5 月 15 日收到修改稿)

建立了跃变参数混沌同步的数学模型,提出并证明了其同步的充分条件,在理论上分析了充分条件的可实现性.提出了跃变参数混沌同步和跃变周期同步的有效算法,借助 Chua 混沌系统仿真实现了参数跃变混沌同步保密通信.最后,分析了跃变参数混沌保密通信对抗现有混沌窃听方法的性能.仿真结果表明跃变参数混沌同步及其保密通信具有易实现和强保密性等优点.

关键词:混沌同步,跃变参数,充分条件,保密通信

PACC:0545

1. 引 言

自 1990 年 PC 同步法及其同步的必要条件[1]提出来后,混沌同步的研究受到学术界的广泛关注[2—9],在这个研究过程中,混沌保密通信[10—12]作为混沌同步的重要应用,一直伴随着混沌同步的研究成为热点课题.而 1998 年 Short 等人利用相图法实现混沌通信窃听的成果[13]公开后,各种混沌通信窃听的方法[14—18]被提出来,证实了即使是高维混沌系统构成的混沌保密通信仍然存在被轻易窃听的可能.在这种研究背景下,迫切需要进一步提出混沌同步的充分条件,并研究更具安全性的混沌保密通信方法.

对于连续动力学系统,主要有二类形式的混沌系统,即分段线性混沌系统和二阶混沌系统.文献[19]针对时不变参数情况,讨论了这二类混沌系统的同步及其实现的充分条件,给出了状态变量的取值空间和严格的证明.本文将进一步研究在参数周期跃变情况下,这二类混沌系统的同步,证明其混沌同步的充分条件,并结合 Chua 系统进行实体电路建模,分析其对抗现有混沌通信窃听方法的性能.

2. 跃变参数混沌同步

定义 M 维跃变参数连续混沌同步系统为驱动系统

$$\frac{\mathrm{d}\boldsymbol{X}(t)}{\mathrm{d}t} = \boldsymbol{f}(\boldsymbol{X}(t), \{u_k(t_0 + nT) \mid k = 1,2,\cdots,H\}); \quad (1)$$

响应系统

$$\frac{\mathrm{d}\boldsymbol{X}'(t)}{\mathrm{d}t} = \boldsymbol{f}(\boldsymbol{X}'(t), \{u'_k(t_0 + nT) \mid k = 1,2,\cdots,H\}) - \boldsymbol{Q}\boldsymbol{W}(\boldsymbol{X}(t) - \boldsymbol{X}'(t)), \quad (2)$$

其中,$\boldsymbol{X}(t) = (x_1(t), x_2(t), \cdots, x_M(t))^{\mathrm{T}} \in R^M$ 为驱动系统的状态向量;$\boldsymbol{X}'(t) = (x'_1(t), x'_2(t), \cdots, x'_M(t))^{\mathrm{T}} \in R^M$ 为响应系统的状态向量;$\boldsymbol{f} = (f_1, f_2, \cdots, f_M)^T$ 为状态向量的演化泛函,使系统为分块线性混沌系统或二阶混沌系统;$u_k(t)$ 和 $u'_k(t)$ 分别表示驱动系统和响应系统的跃变参数在 t 时刻时的取值为第 k 个参数值,$u_k(t)$ 和 $u'_k(t)$ 按周期 T 跃变取值,且取值空间相同;H 为参数跃变取值的总个数;t_0 表示系统起始时刻点;$\boldsymbol{W} \in R^{M\times M}$ 为响应系统的状态观测常数矩阵;$\boldsymbol{Q} \in R^{M\times M}$ 为响应系统的状态反馈常数矩阵.

响应子系统的雅可比矩阵为

$$J_R(\boldsymbol{X}'(t)) = \frac{\mathrm{d}\left(\frac{\mathrm{d}\boldsymbol{X}'(t)}{\mathrm{d}t}\right)}{\mathrm{d}\boldsymbol{X}'(t)} = \frac{\mathrm{d}\boldsymbol{f}(\boldsymbol{X}'(t), u_k)}{\mathrm{d}\boldsymbol{X}'(t)} - \boldsymbol{Q}\boldsymbol{W}, \quad (3)$$

式中,$\mathrm{d}\boldsymbol{f}(\boldsymbol{X}'(t))/\mathrm{d}\boldsymbol{X}'(t) \in R^{M\times M}$ 为 $\boldsymbol{f}(\boldsymbol{X}'(t))$ 的雅可比矩阵,$J_R(\boldsymbol{X}'(t)) \in R^{M\times M}$.

2.1. 跃变参数混沌同步的充分条件

定义 1 由(1)式定义的 M 维动力学系统,J 为

值域，$X(t)\in J$. 给定实正定对角矩阵 $D\in \mathrm{diag}(\lambda_1,\lambda_2,\cdots,\lambda_N)$和正数 $r>0$，把 J 向外扩展到 J'_Z，$J'_Z=\{Z\mid Z\in R^M,\exists X\in J,\mid D(Z-X)\leqslant r\mid\}$. 称 J'_Z 为 J 关于 D 的 r 扩展值域. 包含 J'_Z 的最小非凹扩展值域，记为 $J'_{Dr}(J)$.

当(1)和(2)式中 $u_k(t_0+nT)=u'_k(t_0+nT)=u_0$ 为常数时，(1)和(2)式即为时不变参数混沌同步系统，文献[19]得到了此情况下混沌同步的充分条件定理，引用如下.

引理 1　由(1)和(2)式定义的 M 维混沌同步系统，若其为分段线性混沌系统或二阶混沌系统，值域分别为 J 和 J'. 给定 $r>0$，若存在实正定对角阵 D，当 $X'(t)\in R'_{Dr}(J)\subseteq J'$ 时，有 $D^2(-J_R(X'(t)))$为广义正定阵，且系统初值满足 $X(t_0)\in J$，$\mid D(X(t_0)-X'(t_0))\mid\leqslant r$. 令 $Y(t)=DX(t)$，$Y'(t)=DX'(t)$，系统误差 $S_Y(t)=Y(t)-Y'(t)$，$S_X(t)=X(t)-X'(t)$，则有，$S_Y(t)$和 $S_X(t)$的零解是一致渐近稳定的，且对于任意 $t\in[t_0,+\infty)$，有 $\mathrm{d}\mid S_Y(t)\mid/\mathrm{d}t$ 负定，$X'(t)\in R'_{Dr}(J)$.

定义 2　(1)式的跃变参数混沌驱动系统，对于给定的某组参数 u_k，驱动系统处于混沌态时的值域，称为驱动系统对于 k 的混沌态值域 $R_{ck}(X(t))$. 当驱动系统初值在一定范围内，驱动系统可以演化到混沌态，称此范围为驱动系统对 k 的值域 J_k.

显然有 $R_{ck}(X(t))\subseteq J_k$.

定义 3　对于所有 k，令 $R_c(X(t))=\sum_{k=1}^{H}R_{ck}(X(t))$，$J_0=\prod_{k=1}^{H}J_k$，合理选择参数 u_k，使 $R_c(X(t))\subseteq J_0$，称 $R_c(X(t))$ 为驱动系统的混沌态值域.

显然，当 $X(t_0)\in R_c(X(t))\subseteq J_0$，驱动系统式(1)可以演化到混沌态. 对于所有选定参数 u_k，以及任意初值 $X(t_0)\in R_c(X(t))$，存在一个演化到混沌态的最长过渡时间 T_0，当 $t\geqslant T_0$ 时，对于任意 $X(t_0)\in R_c(X(t))$，必定有 $X(t)\in R_c(X(t))$.

定义 4　(1)式所示跃变参数混沌驱动系统，对给定的某组参数 u_k，对于所有初值 $X(t_0)\in R_c(X(t))$，$X(t_0)$ 的演化轨迹称为 $X(t_0)$ 对于 k 的限初值值域 $R_k(X(t))$. 显然，$R_{ck}(X(t))\subseteq R_k(X(t))$. 对于所有 k，令 $R(X(t))=\sum_{k=1}^{H}R_k(X(t))$，称 $R(X(t))$ 为 $X(t)$ 的限初值值域.

显然有 $R_c(X(t))\subseteq R(X(t))$.

定义 5　给定实正定对角阵 D 和正数 r，将 $R(X'(t))$按定义 1 扩展得到 $R'_{Dr}(X'(t))$，且 $X'(t)$ 在 $R_{Dr}(X'(t))$内有定义，称 $R'_{Dr}(X'(t))$为响应系统(2)式对所有参数 u_k 关于 D 的 r 非凹扩展值域.

定理 1　对于(1)和(2)式定义的跃变参数混沌同步系统，给定实正定对角阵 D 和正数 r，当 $X'(t)\in R'_{Dr}(X'(t))$，对每组跃变参数 u_k，均有 $D^2(-J_R(X'(t)))$广义正定，且初值满足 $X(t_0)\in R_c(X(t))$，$\mid D(X(t_0)-X'(t_0))\mid\leqslant r$. 令 $Y(t)=DX(t)$，$Y'(t)=DX'(t)$，系统误差 $S_Y=Y(t)-Y'(t)$，$S_X(t)=X(t)-X'(t)$. 则有，$S_Y(t)$和 $S_X(t)$的零解是渐近稳定的，且对于任意 $t\in[t_0,+\infty)$，$\mathrm{d}\mid S_Y(t)\mid/\mathrm{d}t$负定，$X'(t)\in R'_{Dr}(X'(t))$.

证明　由(1)和(2)式组成的混沌同步系统演化的第一个周期内，即 $n=1$ 时，参数 u_i 保持恒定值，这时，对于 $\forall\, t\in[t_0,t_0+T)$，有 $X(t)\in R_c(X(t))$，同步系统满足引理 1 的条件，所以，$\frac{\mathrm{d}\mid S_Y(t)\mid}{\mathrm{d}t}<0$. 于是，$\forall\, t\in[t_0,t_0+T)$，$\mid D(X(t)-X'(t))\mid<r$，$X'(t)\in R_{cDr}(X'(t))$.

在第一个周期末，$t=t_0+T$，参数 u_i 跃变为 u_j，由于动力系统状态连续，状态向量值不会跃变，即 $X(t_0+T+0^-)=X(t_0+T+0^+)\in R_c(X(t))$，$X'(t_0+T+0^-)=X'(t_0+T+0^+)\in R_{cDr}(X'(t))$.

在第二个周期内，即 $n=2$，同步系统也满足引理 1 的条件，即 $\forall\, t\in[t_0+T,t_0+2T)$，有 $\frac{\mathrm{d}\mid S_Y(t)\mid}{\mathrm{d}t}<0$，$X(t)\in R_c(X(t))$，$X'(t)\in R_{cDr}(X'(t))$.

由数学归纳法，依此类推，以后的每个周期内，都有 $\frac{\mathrm{d}\mid S_Y(t)\mid}{\mathrm{d}t}<0$，$X(t)\in R_c(X(t))$，$X'(t)\in R_{cDr}(X'(t))$. 于是，$\forall\, t\in[t_0,+\infty)$，有 $\frac{\mathrm{d}\mid S_Y(t)\mid}{\mathrm{d}t}<0$，$X(t)\in R_c(X(t))$，$X'(t)\in R_{cDr}(X'(t))$.

选取 Lyapunov 泛函为 $V(t)=\mid S_Y(t)\mid$，于是，$\forall\, t\in[t_0,+\infty)$，$V(t)$正定，$\frac{\mathrm{d}V(t)}{\mathrm{d}t}<0$，且 $X(t)\in R_c(X(t))$，$X'(t)\in R_{cDr}(X'(t))$有界.

综上，可得系统误差 $S_Y(t)$和 $S_X(t)$的零解是渐近稳定的，且对于 $\forall\, t\in[t_0,+\infty)$，有 $\frac{\mathrm{d}\mid S_Y(t)\mid}{\mathrm{d}t}<0$，$X'(t)\in R_{cDr}(X'(t))$有界.

由定理 1 的证明可知，如果对于任选的某个周

期内,定理 1 的条件得到满足,则对于该周期以后的所有时间内,定理 1 的条件同样可以满足.这里任选第 n 个周期,跃变参数值固定为 u_i,设混沌同步系统为 M 维动力学系统,选取 $\boldsymbol{QW}=\mathrm{diag}(k_1,k_2,\cdots,k_M)$为正定对角阵,

$$\frac{1}{2}((J_R(X(t)))^{\mathrm{T}}+J_R(X(t)))=\frac{1}{2}\left(\left(\frac{\mathrm{d}\boldsymbol{f}(\boldsymbol{X}(t))}{\mathrm{d}\boldsymbol{X}(t)}\right)^{\mathrm{T}}+\frac{\mathrm{d}\boldsymbol{f}(\boldsymbol{X}(t))}{\mathrm{d}\boldsymbol{X}(t)}\right)-\boldsymbol{QW},\quad(4)$$

记$\frac{\mathrm{d}\boldsymbol{f}(\boldsymbol{X}(t))}{\mathrm{d}\boldsymbol{X}(t)}=[a_{ij}]_{M\times M}$,$a_{ij}\in R$,由于混沌同步系统的 J 有界,给定正定阵 $\boldsymbol{D}$ 和正实数 r,使 $R'_{Dr}(J)\subset J'$,有 $R'_{Dr}(J)$有界,因此,a_{ij}有界.于是,当

$$k_i>\frac{1}{2}\Big(\sum_{j=1,j\neq i}^{M}|a_{ij}+a_{ji}|\Big)-a_{ii},\ i,j=1,2,\cdots,M\quad(5)$$

时,由特征值的圆盘定理可知,$\frac{1}{2}((J_R(X(t)))^{\mathrm{T}}+J_R(X(t)))$的所有特征值都小于 0,即 $-J_R(X'(t))$广义正定,所以,$\boldsymbol{D}^2(-J_R(X'(t)))$也广义正定.选取初值 $X(t_0+(n-1)T)\in J$,$|\boldsymbol{D}(X(t)-X'(t))|\leqslant r$,就可以满足第 n 个周期的充分条件,从而可以满足 $t\in[t_0+nT,+\infty)$时定理 1 的条件.一般地,可以通过调整矩阵 $\boldsymbol{D}$,使 $\boldsymbol{QW}$ 取较小的值时,$\boldsymbol{D}^2(-J_R(X'(t)))$就广义正定,这样系统同步比较容易实现.

2.2. 跃变参数混沌同步通信算法

在(1)和(2)式组成的跃变参数混沌同步系统基础上,可以采用混沌掩蔽、混沌开关、混沌调制或混沌键控等多种形式进行混沌保密通信.这里将有用信号 $I(t)$调制到驱动系统的一个非跃变的时变参数 $u_0(t)$上,建立如下的驱动——响应同步通信系统.

驱动系统

$$\frac{\mathrm{d}\boldsymbol{X}(t)}{\mathrm{d}t}=\boldsymbol{f}(\boldsymbol{X}(t),u_0(t),\{u_i(t_0+nT)\mid i=1,2,\cdots,H\});\quad(6)$$

响应系统

$$\begin{aligned}\frac{\mathrm{d}\boldsymbol{X}'(t)}{\mathrm{d}t}&=\boldsymbol{f}(\boldsymbol{X}'(t),u'_0(t),\{u'_i(t_0+nT)\mid i=1,2,\cdots,H\})-\boldsymbol{QW}(\boldsymbol{X}(t)-\boldsymbol{X}'(t)),\\\frac{\mathrm{d}u'_0(t)}{\mathrm{d}t}&=g\boldsymbol{W}(\boldsymbol{X}(t)-\boldsymbol{X}'(t));\end{aligned}\quad(7)$$

(6)和(7)式中,$u_0(t)$为驱动系统中非跃变的时变参数,$u'_0(t)$为响应系统中对 $u_0(t)$的估计,g 为增益常数,其他符号说明同前.

(7)式的雅可比矩阵为

$$\boldsymbol{J}=\begin{pmatrix}\dfrac{\partial\boldsymbol{f}(\boldsymbol{X}'(t),u'_0(t),\{u'_i(t_0+nT)\})}{\partial\boldsymbol{X}'(t)}+\boldsymbol{QW} & \dfrac{\partial\boldsymbol{f}(\boldsymbol{X}'(t)u'_0(t),\{u'_i(t_0+nT)\})}{\partial u'_0(t)}\\ \dfrac{\partial g\boldsymbol{W}(\boldsymbol{X}(t)-\boldsymbol{X}'(t))}{\partial\boldsymbol{X}'(t)} & \dfrac{\partial g\boldsymbol{W}(\boldsymbol{X}(t)-\boldsymbol{X}'(t))}{\partial u'_0(t)}\end{pmatrix},\quad(8)$$

(8)式中,$\frac{\partial\boldsymbol{f}(\boldsymbol{X}'(t),u'_0(t),\{u'_i(t_0+nT)\})}{\partial\boldsymbol{X}'(t)}\in R^{M\times M}$,$\frac{\partial\boldsymbol{f}(\boldsymbol{X}'(t),u'_0(t),\{u'_i(t_0+nT)\})}{\partial u'_0(t)}\in R^{M\times 1}$,$\frac{\partial g\boldsymbol{W}(\boldsymbol{X}(t)-\boldsymbol{X}'(t))}{\partial\boldsymbol{X}'(t)}\in R^{1\times M}$,$\frac{\partial g\boldsymbol{W}(\boldsymbol{X}(t)-\boldsymbol{X}'(t))}{\partial u'_0(t)}\in R^{1\times 1}$.

显然,当 $u_0(t)$为常数且不调制有用信号时,由引理 1 和定理 1 可以保证系统能够建立同步,这里由于引入了时变参数 $u_0(t)$,并且在其上调制了有用信号 $I(t)$,还需要计算(8)式决定的条件 Lyapunov 指数(CLE)是否小于 0,保证系统在经过一段过渡时间后进入混沌同步态.

根据需要选定跃变参数的跃变周期 T.

定义 6 定义响应系统单周期不同步时间为

$$\Gamma_T(n)=\frac{1}{2}\int_{t_r(n)}^{t_r(n)+T}(\mathrm{sgn}(|\boldsymbol{X}(t)-\boldsymbol{X}'(t)|^2-l_1)+1)\mathrm{d}t,\quad(9)$$

其中,$t_r(n)$为响应系统第 n 个跃变周期的起始时刻,$\mathrm{sgn}(\cdot)$为符号函数,l_1 为选取的同步门限,同步时有 $|\boldsymbol{X}(t)-\boldsymbol{X}'(t)|^2\leqslant l_1$.由于跃变参数不同步时

状态向量差值较大，l_1 应取较大值，以突出对参数不同步的估计．$\Gamma_T(n)$ 表示响应系统第 n 个跃变周期内系统状态向量间的不同步时间．

定义 7　定义响应系统周期末不同步时间为

$$\Gamma_h(n) = \frac{1}{2}\int_{t_r(n)+T-h}^{t_r(n)+T} (\mathrm{sgn}(|\boldsymbol{X}(t) - \boldsymbol{X}'(t)|^2 - l_1) + 1)\mathrm{d}t, \quad (10)$$

其中，$h \ll T$，$\Gamma_h(n)$ 表示在响应系统的第 n 个跃变周期末尾 h 长的时段内系统的不同步时间．

定义 8　定义整周期不同步时间门限为 Γ_{TT}，$\Gamma_{TT} \leqslant T$；定义整周期同步时间门限为 Γ_{T0}，$\Gamma_{T0} \gg 0$；定义周期末不同步时间门限为 Γ_{h0}，$\Gamma_{h0} \geqslant 0$．于是当 $\Gamma_T(n) \geqslant \Gamma_{TT}$ 时，则认为响应系统第 n 个跃变周期内均不同步；当 $\Gamma_T(n) \geqslant \Gamma_{T0}$ 时，认为响应系统第 n 个跃变周期内存在不同步；当 $\Gamma_T(n) < \Gamma_{T0}$ 时，认为响应系统第 n 个跃变周期内同步．

定义 9　在响应系统与驱动系统的跃变参数完全相同情况下，系统由不同的初值达到完全同步的时间，定义为参数匹配同步暂态时间 Γ_{s0}．一般通过计算 N 次单周期不同步时间 $\Gamma_T(n)$，求平均值得到 Γ_{s0}，所以 Γ_{s0} 与 Γ_{T0} 的取值很接近，

$$\Gamma_{s0} = \frac{1}{2N}\sum_{i=1}^{N}\int_{t_r(n)}^{t_r(n)+T} (\mathrm{sgn}(|\boldsymbol{X}(t) - \boldsymbol{X}'(t)|^2 - l_1) + 1)\mathrm{d}t. \quad (11)$$

如果响应系统与驱动系统间存在着跃变周期部分不同步，即 $\Gamma_T(n) \geqslant \Gamma_{T0}$ 且 $\Gamma_T(n) < \Gamma_{TT}$，记第 n 个跃变周期驱动信号 $X(t)$ 的起始时刻为 $t_s(n)$，响应系统起始时刻为 $t_r(n)$，则有 $|t_s(n) - t_r(n)| = \Gamma_T(n) - \Gamma_{s0}$，即第 n 个跃变周期驱动和响应状态向量错位的时间等于不同步时间 $\Gamma_T(n)$ 与参数匹配同步暂态时间 Γ_{s0} 的差，显然，$\Gamma_T(n) \geqslant \Gamma_{s0}$．此时，若周期末不同步时间 $\Gamma_h(n) > 0$，表明在响应系统的第 n 个跃变周期末不同步，又由于 $\Gamma_T(n) < \Gamma_{TT}$，所以，此时响应系统跃变周期比驱动系统滞后．反之，当 $\Gamma_h(n) = 0$，表明响应系统跃变周期比驱动系统超前．

响应系统在第 n 个跃变周期采样数据，在随后的 k 个跃变周期内完成数据处理，在第 $n+k+1$ 个跃变周期内进行跃变周期调整，把响应系统跃变周期滞后 Δt，使

$$t_s(n+k+1) - t_r(n+k+1) = 0, \quad (12)$$

从而使同步系统跃变周期同步．

由于

$$\begin{aligned} & t_s(n+k) - t_r(n+k) \\ &= t_s(n) + kT - (t_r(n) + kT) \\ &= t_s(n) - t_r(n), \end{aligned} \quad (13)$$

故

$$\begin{aligned} \Delta t &= -(t_s(n) - t_r(n)) \\ &= (2\mathrm{sgn}(\Gamma_h(n)) - 1)(\Gamma_T(n) - \Gamma_{s0}), \end{aligned} \quad (14)$$

因此，响应系统在第 $n+k+1$ 个跃变周期把周期起始时刻滞后 Δt，就可以使同步系统跃变周期同步．

在第 n 个跃变周期，当响应系统单周期不同步时间 $\Gamma_T(n) < \Gamma_{T0}$ 时，可认为同步系统处于跃变周期同步状态，不需要调整；当响应系统单周期不同步时间 $\Gamma_T(n) > \Gamma_{TT}$ 时，表明系统不同步超过一个跃变周期，需要重新建立同步．

在上面分析的基础上，建立跃变参数同步通信有以下具体步骤：

1）选取适当的 Γ_{TT}，Γ_{T0} 和 Γ_{h0}，依经验估算 Γ_{s0}．

2）在系统开始建立同步的时候，驱动系统和响应系统的跃变参数 $u_i(t) = u_i'(t)$，且固定不变．驱动系统把有用信号 $I(t)$ 调制在参数 $u_0(t)$ 中，发出约定的有用信号 $I(t)$ 以请求同步，此时的 $I(t)$ 以跃变周期 T 变化，即 $I(t) = I(t_0 + nT)$，让响应系统接收并解调出 $I(t_0 + nT)$，从而知道跃变周期的起始时刻 t_0，并记下周期 T 的大小，从而建立起同步．

3）同步建立后，就可以进行跃变参数混沌同步保密通信．在通信过程中，由于环境变化及多径效应等的影响，会使响应系统的跃变周期起始位置发生变化，从而造成响应系统的跃变周期与驱动系统失步．此时，对响应系统每个参数跃变周期计算 $\Gamma_T(n)$，并与 Γ_{T0} 比较，分以下三种情况进行处理：

（i）当 $\Gamma_T(n) < \Gamma_{T0}$ 时，表明整周期不同步在允许范围内，对跃变周期不做调整．

（ii）当 $\Gamma_T(n) \geqslant \Gamma_{T0}$ 且 $\Gamma_T(n) < \Gamma_{TT}$ 时，对此周期计算 $\Gamma_h(n)$ 以及（14）式定义的 Δt，在随后的 k 个跃变周期内作数据处理，并把响应系统第 $n+k+1$ 个跃变周期的起始时刻滞后 Δt，随后的跃变周期以此时刻为起始点．

（iii）当 $\Gamma_T(n) \geqslant \Gamma_{T0}$ 且 $\Gamma_T(n) > \Gamma_{TT}$ 时，此时第 n 个跃变周期整周期均不同步．接下来连续检验二个跃变周期，若都有 $\Gamma_T(n) > \Gamma_{TT}$，则响应系统向驱动系统发送重新建立同步信号，以请求重新建立同步．随后切换到步骤 1）重新建立同步．一般地，这种

情况在合理选择 T 的情况下较少发生.

3. 跃变参数混沌同步通信的 Chua 电路实现

以 Chua 电路[20,21]为基础的跃变参数混沌同步通信的实现框图如图 1 所示.

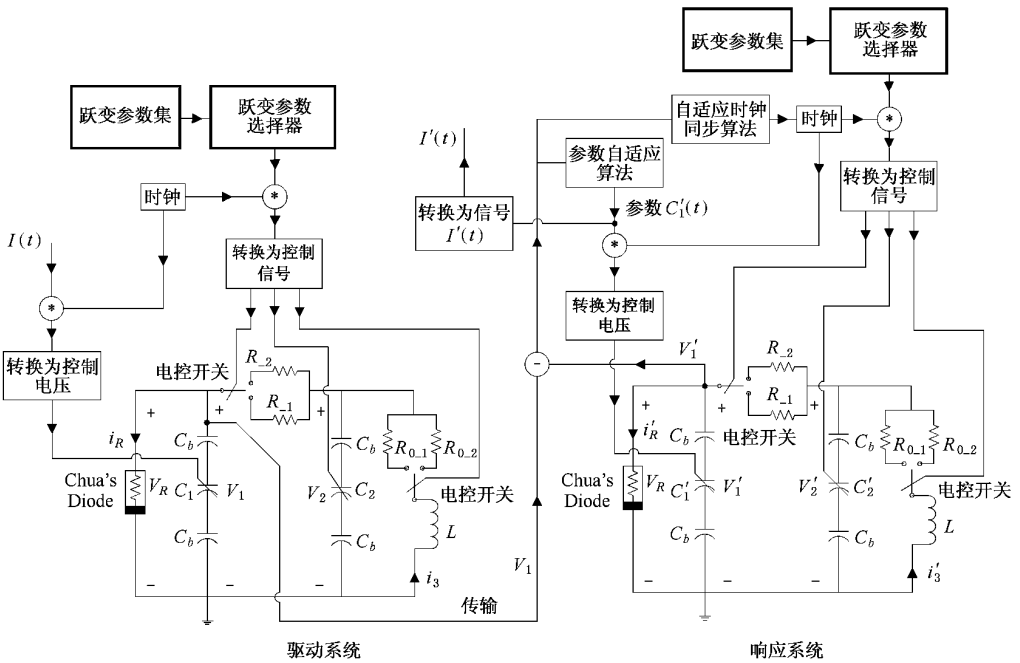

图 1 建立在 Chua 电路上的跃变参数混沌同步保密通信实现框图

$$\frac{\mathrm{d}V_1(t)}{\mathrm{d}t} = \frac{1}{C_1(t)}[G(t_0+nT)(V_2(t) - V_1(t)) - f(V_1(t))],$$

$$\frac{\mathrm{d}V_2(t)}{\mathrm{d}t} = \frac{1}{C_2(t_0+nT)}[G(t_0+nT)(V_1(t) - V_2(t)) + i_3(t)],$$

$$\frac{\mathrm{d}i_3(t)}{\mathrm{d}t} = \frac{1}{L}[-V_2(t) - R_0(t_0+nT)i_3(t)], \quad (15)$$

其中,$G=1/R$,C_2 和 R_0 为跃变参数,C_1 作为传输信息调制参数,$\frac{1}{C_1(t)} = \frac{I(t)}{C_{10}}$,$C_{10}$ 为正常数,$I(t)$ 为传输的有用信息,这里为 0 或 1 二相编码信号.

$$f(V_1(t)) = G_bV_1(t) + \frac{1}{2}(G_b - G_a)(|V_1(t) + E| - |V_1(t) - E|), \quad (16)$$

(16)式中 G_a,G_b 和 E 为适当的常数,反映了 Chua 电路二极管的伏安特性.

响应系统为

$$\frac{\mathrm{d}V_1'(t)}{\mathrm{d}t} = \frac{1}{C_1'(t)}[G'(t_r+nT)(V_2'(t) - V_1'(t)) - f(V_1'(t)) + K_1(V_1(t) - V_1'(t))],$$

$$\frac{\mathrm{d}V_2'(t)}{\mathrm{d}t} = \frac{1}{C_2'(t_r+nT)}[G'(t_r+nT)(V_1'(t) - V_2'(t)) + i_3'(t) + K_1(V_1(t) - V_1'(t))],$$

$$\frac{\mathrm{d}i_3'(t)}{\mathrm{d}t} = \frac{1}{L}[-V_2'(t) - R_0'(t_r+nT)i_3'(t) + K_1(V_1(t) - V_1'(t))],$$

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = K_{c1}\mathrm{sgn}[G'(t_r+nT)(V_2'(t) - V'_1(t)) - f(V'_1(t)) + K_1(V_1(t) - V_1'(t))](V_1(t) - V_1'(t)),$$

$$\frac{1}{C_1'(t)} = \frac{I(t)}{C_{10}}, \quad (17)$$

其中,K_1 为反馈系数,$K_1=0.001$;K_{c1} 为收敛因子,$L=7.14\times10^{-3}$ H,$G_a=-0.8\times10^{-3}$ S,$G_b=-0.5\times$

10^{-3}S，$E=1$V.

对于相应的跃变周期 n，驱动和响应系统的跃变参数 $G=G'$，$C_2=C_2'$，$R_0=R_0'$. 跃变参数作为密钥，其变化规律应具有无序性、非周期性和难以预测性. 这里，$R_0=R'_0$ 随 n 做无规律的 0 和 10 二值变化，$G=G'$ 随 n 做无规律的 0.67×10^{-3} 和 0.70×10^{-3} 二值变化，$C_2=C_2'$ 随 n 在 $[5.0\times10^{-8},6.5\times10^{-8}]$ 的连续区间内做随机跃变. 实际通信系统中还可以采用其他形式的跃变参数变化规律.

按第 2.2 节介绍的方法，对图 1 所示跃变参数混沌同步通信系统进行仿真.

1）混沌同步的建立

驱动和响应系统的跃变参数设为相等，即 $G=G'$，$C_2=C'_2$，$R_0=R_0'$ 为约定值并且保持不变，这里取 $G=G'=0.75\times10^{-3}$，$C_2=C_2'=0.8\times10^{-7}$，$R_0=R_0'=12$. 约定传输信号 $I(t)$ 出现 10011010 时，认为响应系统和驱动系统已经完成跃变周期及其参数的同步，响应系统以解调出的信号 $I'(t)$ 的变化起始时刻作为跃变周期的起始时刻. 在这之后第 w 个时钟（响应系统在此期间做同步应答）的起始时刻，驱动系统开始向响应系统（接收方）发送需要通信的有用信号 $I(t)$，即这时才开始保密通信. 此时，驱动系统或响应系统的吸引子如图 2 所示，同步通信系统的仿真结果如图 3 所示.

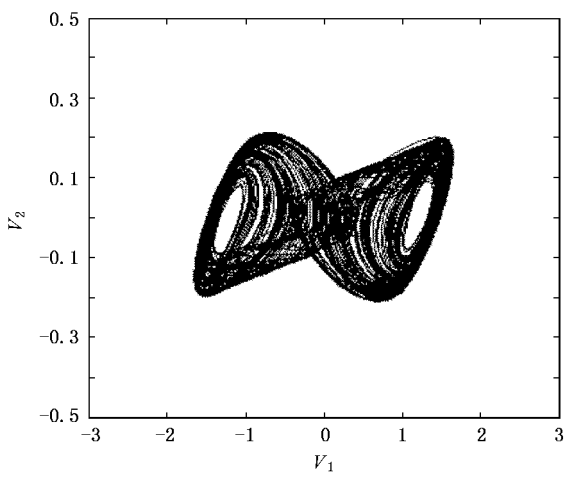

图 2　驱动系统或响应系统的吸引子

从图 3 可以看出，在建立同步时 $I(t)$ 很容易被响应系统接收到，并以 $I'(t)$ 恢复出来. 响应系统从 $I'(t)$ 中出现的 10011010，得知第 1 个跃变参数跃变周期的起始时刻，进而同步以后的跃变周期.

2）建立同步后的保密通信

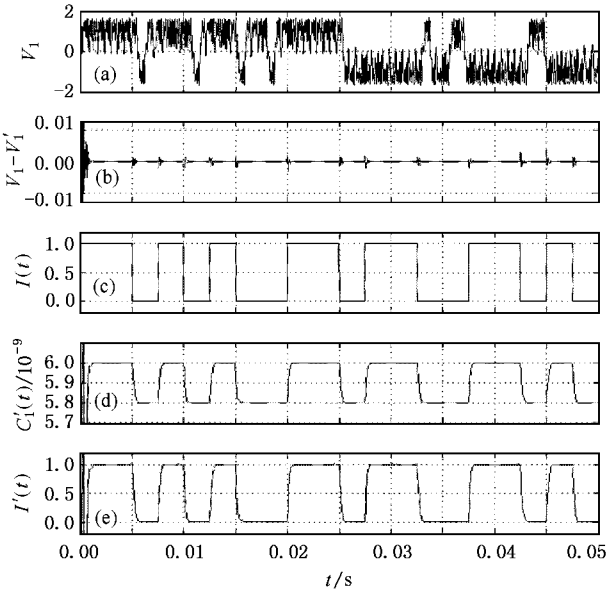

图 3　跃变参数混沌保密通信同步的建立. (a)驱动信号 V_1；(b)驱动信号与响应信号之差 $V_1-V'_1$；(c)传输的信号 $I(t)$；(d)响应方解调出的参数 $C_1'(t)$；(e)响应方恢复出的信号 $I'(t)$

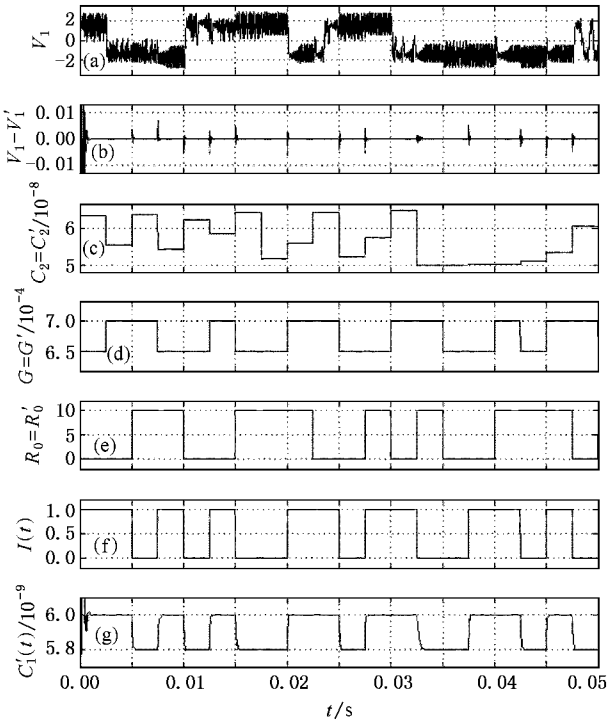

图 4　跃变参数混沌保密通信的仿真图. (a)驱动信号 V_1；(b)驱动信号与响应信号之差 $V_1-V'_1$；(c)跃变密钥参数 $C_1(t)=C'_1(t)$；(d)跃变密钥参数 $G=G'$；(e)跃变密钥参数 $R_0=R_0'$；(f)传输的信号 $I(t)$；(g)响应方解调出的参数 $C_1'(t)$

驱动和响应系统的跃变参数对于相应的跃变周

期 n，有 $G=G'$，$C_2=C'_2$，$R_0=R'_0$，并且随 n 的步进按双方约定的规律随机变化.这里，取 $R_0=R'_0$ 随 n 做 0 和 10 二值随机变化，$G=G'$ 随 n 做 0.67×10^{-3} 和 0.70×10^{-3} 二值随机变化，$C_2=C'_2$ 随 n 在 $[5.0\times10^{-8},6.5\times10^{-8}]$ 的连续区域内做跃变.同步后保密通信的仿真结果如图 4 所示，跃变参数混沌同步保密通信在同步建立后，通信是成功的.

3)失步检测

如果由于环境变化和多径效应等的影响，跃变参数跃变周期在响应系统和驱动系统间发生了错位，这时采用第 2.2 节的同步算法恢复跃变参数周期同步.当跃变参数周期突然错位 1 个跃变周期以上，且连续 3 个跃变周期都是如此，则按第 2.2 节方法重新建立混沌同步.仿真时发现，在合理选择 T 的情况下，很少会发生跃变周期突然错位超过 1 个跃变周期，一般的周期错位往往在 1 个跃变周期以内，这时自适应同步算法可以使跃变周期恢复同步.这里仿真了当驱动信号跃变周期相对于响应信号突然滞后 $0.6T$ 或超前 $0.4T$ 的情况下，通过同步算法使跃变周期达到同步，使周期错位达到允许门限以下，如图 5 和 6 所示.

图 5 和 6 的同步算法是按这种方式进行的，即响应系统在第 n 个跃变周期完成采样，第$(n+1)$个跃变周期进行数据处理，第$(n+2)$个跃变周期内进行周期调整，第$(n+3)$个跃变周期又采样，……，如此循环进行.从图 5 和 6 中可以看出，同步算法是很有效的，使跃变参数周期恢复了同步.

4. 跃变参数混沌同步保密通信的性能分析

目前对混沌同步保密通信窃听的入手点，基本上都是基于混沌同步具有强烈的参数敏感性.在此基础上，运用广义同步法[15—17]、相图法或变形相图法[18]、参数自适应估计法[20—23]以及不动点法[24]等方法对其进行窃听.其中，有些方法对通信系统中混沌系统的结构以及参数进行估计，以达到窃听的效果；而有些方法并不直接破译混沌系统，而是通过不含信息的混沌信号与含有信息的混沌信号相对比，或者直接用含有不同信息的混沌信号相对比，破译出系统传输的信息.

采用跃变参数进行混沌同步保密通信，可以有效地消除这些窃听方法对系统破译的可能，主要有以下原因：

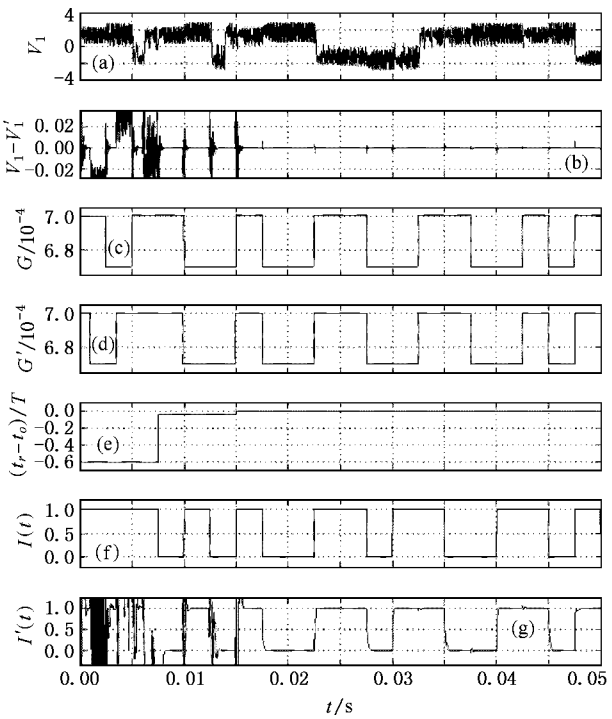

图 5 响应系统跃变参数周期滞后 $0.6T$ 时，通过自适应参数同步算法使之恢复同步的情况.(a)驱动信号 V_1；(b)驱动信号与响应信号之差 $V_1-V'_1$；(c)跃变密钥参数 G；(d) 跃变密钥参数 G'；(e) 参数错位情况；(f) 传输的信号 $I(t)$；(g)接收方恢复出的信号 $I'(t)$

1)同时有多个跃变参数周期性或随机地变化，有效地掩蔽了传输的信息，使之无法直接通过相图的对比破译出传输信号.

2)在跃变参数同步通信过程中，跃变周期起始点的估计，带有很强的继承性，周期本身含有的信息量很少，估计周期所需的信息及时间也很少.而通信双方由于知道跃变参数，因此，估计出传输信息 $I(t)$ 所需的信息很少、时间很短.所以跃变参数周期 T 可以选得比较短.窃听方则不同，其对跃变参数一无所知，要估计出跃变参数及其他信息，需要很多的信息量及时间，而在短短的 T 内，将没有足够的信息量和时间完成对跃变参数的估计.因此，在 T 这段跃变参数不变的时间内估计出所需信息是难以实现的.

3)跃变参数同步通信方法会造成相图混乱，窃听者找不到所谓干净的不含信息的相图，而是大片模糊的区域，无法借助相图提取所含的信息.在同一 T 内，虽然跃变参数不变，但 T 内所含的信息量太少，构不成完整的相图.

下面基于图 1 所示的跃变参数混沌同步通信系

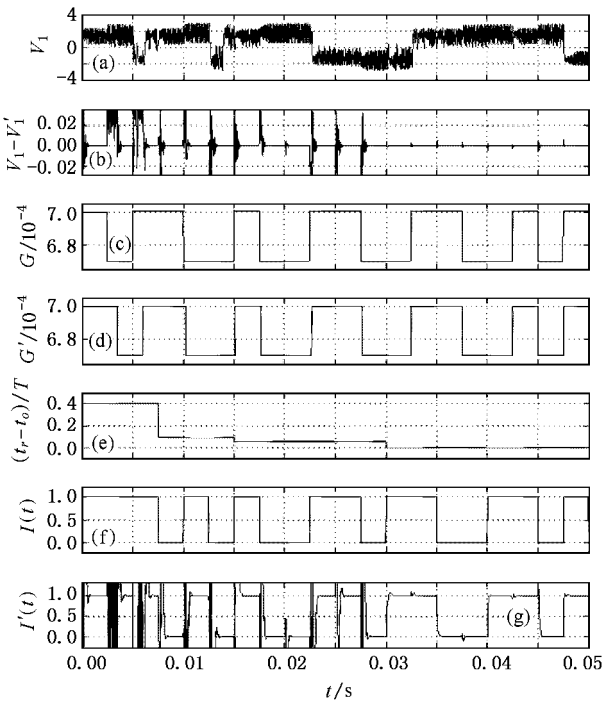

图 6　响应系统跃变参数周期超前 $0.4T$ 时，通过自适应参数同步算法使之恢复同步的情况．(a)驱动信号 V_1；(b)驱动信号与响应信号之差 V_1-V_1'；(c)跃变密钥参数 G；(d) 跃变密钥参数 G'；(e) 参数错位情况；(f) 传输的信号 $I(t)$；(g)接收方恢复出的信号 $I'(t)$

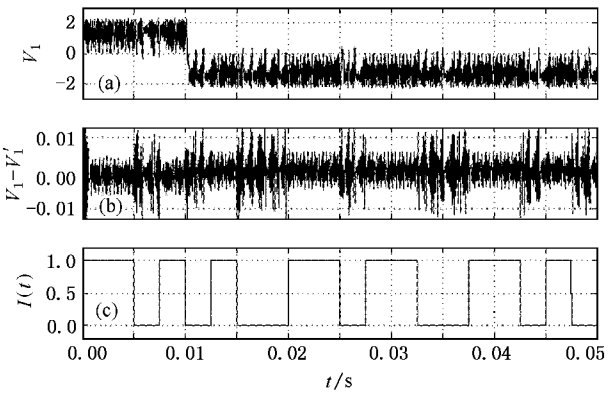

图 7　广义同步法对一般混沌同步通信的窃听　(a)驱动信号 V_1；(b)驱动信号与响应信号之差 V_1-V_1'；(c) 传输的信号 $I(t)$

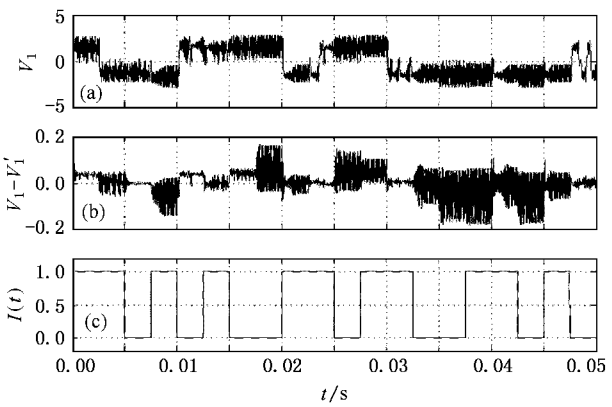

图 8　广义同步法对跃变参数混沌同步通信的窃听　(a)驱动信号 V_1；(b)驱动信号与响应信号之差 V_1-V_1'；(c) 传输的信号 $I(t)$

统讨论其对抗各种解密方法窃听的效果：

1)对抗广义同步法的窃听

广义同步法窃听，是窃听者使用自选的响应系统(结构可以与驱动系统不同)，在不知道驱动系统参数的情况下，选取特定的响应系统参数，与驱动系统形成广义同步，从而破译出所含信息．由于广义同步容易实现，故此窃听方法易于实施．

图 7 表示仅采用一般混沌同步方法，未采用跃变参数法进行混沌保密通信，窃听者采用广义同步进行窃听的情况．可见，窃听者可以通过同步误差的波形解调出所需信息．图 8 表示采用跃变参数法进行通信，窃听者用广义同步法窃听的情况，由于 $I(t)$ 被时变参数所掩蔽，窃听者无法解调出有用信息．

2)对抗相图及变形相图法的窃听

相图法或变形相图法的窃听，是利用含有不同信息的混沌信号，在相图或变形相图(比如回归映射相图)上，呈现出不同的位置及形状特点，通过度量这些差异，破译出所含的信息．由于跃变参数混沌同步通信的传输信息 $I(t)$ 被时变参数掩蔽，并且有些跃变参数在连续区域上取值，在相图上根本无法识别哪些是跃变参数引起的差异，哪些是有用信号 $I(t)$ 引起的差异，因此，更谈不上破译信息．再者，窃听者找不到不含信息的相图(或信息 $I(t)$ 为 0)作为基准，因为，对于每种不同跃变参数的组合，就有一种某种意义上的基准，而跃变参数不同取值的组合数趋近于无穷大，因此基准也是无穷多的，也就失去了基准的意义，因而无法用基准来破译信息．虽然跃变参数在一个跃变周期 T 内不变，但 T 内所含混沌信息太少，构成相图的点太少，从而也无法利用相图进行破译．

图 9 和 10 所示仿真采用文献[18]的方法．定义 M_n 为 $X(t)$ 的第 n 个极大值，I_n 为 $X(t)$ 的第 n 个极小值，令 $A_n=(M_n+I_n)/2$，$B_n=M_n-I_n$，$C_n=(M_{n+1}+I_n)/2$，$D_n=I_n-M_{n+1}$，把 A_n 与 B_n 和 $-C_n$ 与 $-D_n$ 画在同一张相图上就得到图 9 和 10 所示的相图．

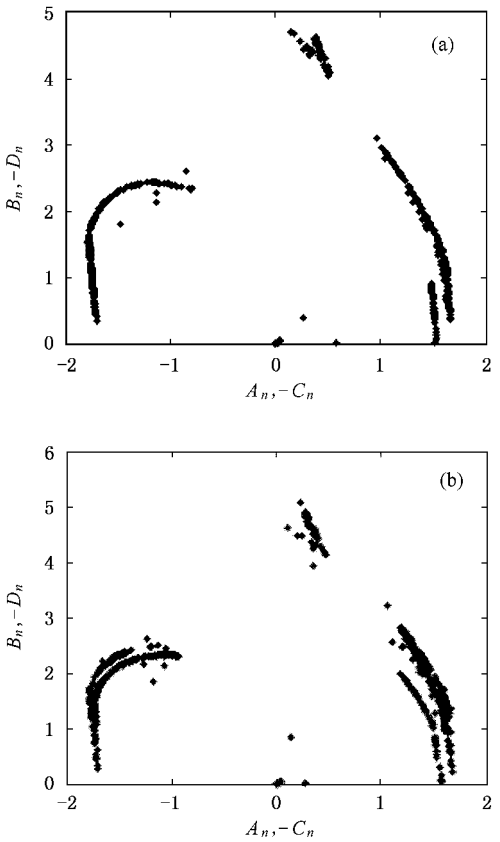

图 9 一般混沌同步通信面对回归相图法的窃听 (a)只含信息 $I(t)=0$ 的基准相图;(b)通信时 $I(t)$ 为 0 和 1 二值信息的相图

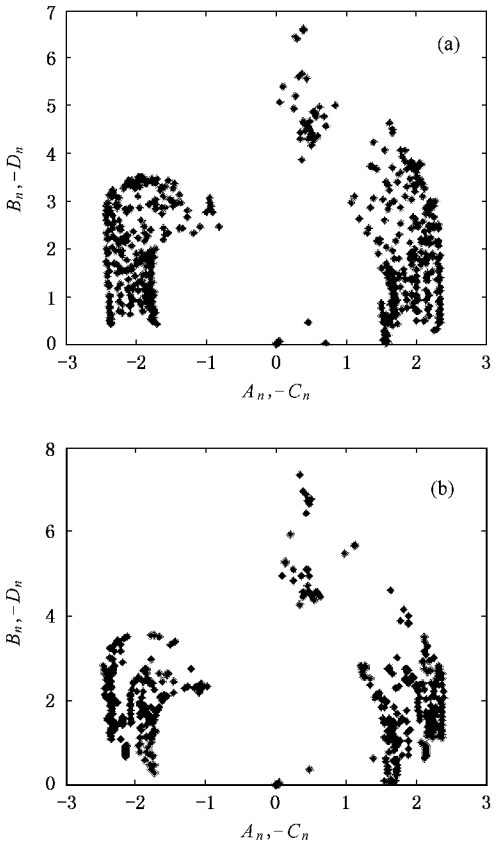

图 10 时变密钥参数混沌同步通信面对回归相图法的窃听 (a)只含信息 $I(t)=0$ 的基准相图;(b)通信时 $I(t)$ 为 0 和 1 二值信息的相图

从图 9 可以看出,对于一般混沌同步通信,不含信息(或只含信息 0)的基准相图比较清晰,含有信息的相图与之相比有明显差异,通过对比某些时刻的点与基准相图的异同,窃听者可以解密传输的信息.而从图 10 可以得知,跃变参数混沌同步通信的不含信息(或只含信息 0)的基准相图是一片模糊的区域,不能作为基准,含 $I(t)$ 的相图与之对比也得不到有用的信息,窃听者也就无从破译信息.

3)对抗参数自适应估计法的窃听

参数自适应估计法的窃听,是窃听者知道混沌系统结构的情况下,利用参数自适应算法来估计混沌系统的参数,从而破解出所传输的信息.对于跃变参数混沌保密通信,由于窃听方未知的参数比通信方多得多,在短短的跃变周期 T 内,通信方可以估计出信息参数,而窃听方则无法估计出所需参数.图 11 和 12 分别表示未采用跃变参数通信和采用跃变参数通信的情况下,用参数自适应算法窃听的结果.可以看出,未采用跃变参数的混沌同步保密通信被窃听了,采用了跃变参数的保密通信无法被窃听.

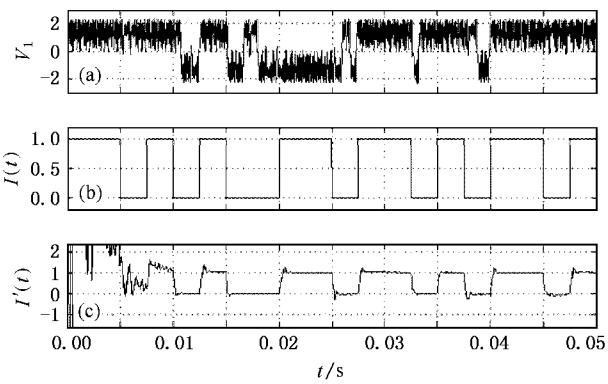

图 11 参数自适应估计法对一般混沌同步通信的窃听 (a)驱动信号 V_1;(b) 传输的信号 $I(t)$;(c) 窃听方恢复出来的信号 $I'(t)$

4)对抗不动点法的窃听

不动点法的窃听,要求窃听者不仅预知通信双方混沌系统的结构,而且能够进入到通信系统内部,通过向响应系统的输入端输入常数,使得接收方混沌系统的状态变量收敛到常数,根据输入的常数以

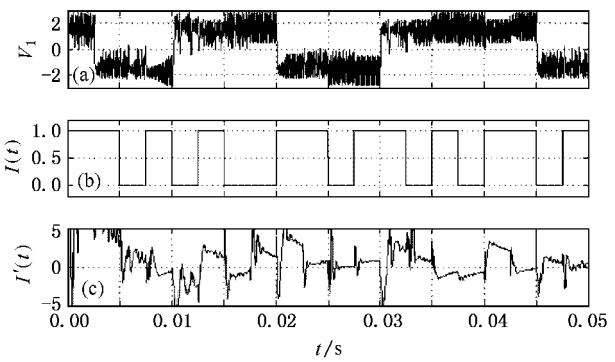

图 12　参数自适应估计法对跃变参数混沌同步通信的窃听 (a)驱动信号 V_1；(b) 传输的信号 $I(t)$；(c) 窃听方恢复出来的信号 $I'(t)$

及对应的状态变量的常数值，破解出混沌系统的参数，这对窃听者的要求是很高的.这种方法对跃变参数混沌同步通信系统显然是无效的，在正确保管好跃变参数集的前提下，非有用信息传输的通信时段内，跃变参数混沌通信系统中的跃变参数是非密钥的常态值，既使这段时间内窃听者能够获得这些常态值，但当传输有用信号的通信过程中跃变参数将周期性或随机地跃变，这些常态参数对窃听有用信息根本没有帮助.

5. 结　论

本文在文献[19]的基础上，提出了跃变参数混沌同步的方法及其充分条件，并证明了充分条件及其可行性，提出了跃变参数混沌同步和跃变周期同步的算法，借助于 Chua 混沌电路给出了跃变参数混沌同步保密通信的实现原理图，仿真证实了跃变参数混沌同步及其周期同步的可行性，最后讨论了跃变参数混沌保密通信对抗现有混沌窃听方法的性能，充分说明了跃变参数混沌保密通信具有保密性强、操作容易等优点，具有较强的理论和应用研究价值.目前，我们正在开展跃变参数混沌保密通信的硬件实现研究，在进一步的理论研究中，将针对时变参数多维混沌系统同步，论证其同步的充分条件及其保密通信性能.

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

[2] Luo X S, Fang J Q, Wang L H, Kong L J, Weng J Q 1999 *Acta Phys. Sin.* **48** 2022 (in Chinese) [罗晓署、方锦清、王力虎、孔令江、翁甲强 1999 物理学报 **48** 2022]

[3] Li L X, Peng H P, Lu H B 2001 *Acta Phys. Sin.* **50** 629 (in Chines) [李丽香、彭海朋、卢辉斌 2001 物理学报 **50** 629]

[4] Liu F C, Wang J, Peng H P 2002 *Acta Phys. Sin.* **51** 1954 (in Chinese) [刘福才、王　娟、彭海朋 2002 物理学报 **51** 1954]

[5] Uchida A, McAllister R, Meucci R 2003 *Phys. Rev. Lett.* **91** 174101

[6] Pastur L, Boccaletti S, Ramazza P L 2004 *Phys. Rev.* E **69** 36201

[7] Gao X, Yu J B 2005 *Chin. Phys.* **14** 908

[8] Yue L J, Shen K 2005 *Chin. Phys.* **14** 1760

[9] Lu J G 2006 *Chin. Phys.* **15** 83

[10] Kolumb 'an G, Kennedy M P, Chua L O 1998 *IEEE Trans. Circuits Syst.* I **45** 1129

[11] Zhang J S, Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese) [张家树、肖先赐 2001 物理学报 **50** 2121]

[12] Zhou Y, Wu L, Zhu S Q 2005 *Chin. Phys.* **14** 2196

[13] Short K M, Parker A T 1998 *Phys. Rev.* E **58** 1159

[14] Zhou C S, Lai C H 1999 *Phys. Rev.* E **60** 320

[15] Rulkov N F, Sushchik M M, Tsimring L S 1995 *Phys. Rev.* E **51** 980

[16] Kocarev L, Parlitz U 1996 *Phys. Rev. Lett.* **76** 1816

[17] Yang T, Yang L B, Yang C M 1998 *IEEE Trans. Circuits Syst.* I **45** 1062

[18] Perez G 1995 *Phys. Rev. Lett.* **74** 6253

[19] Chen B, Liu G H, Zhang Y, Zhou Z O 2005 *Acta Phys. Sin.* **54** 5039 (in Chinese) [陈　滨、刘光祜、张　勇、周正欧 2005 物理学报 **54** 5039]

[20] Yang T, Chua L O 1996 *IEEE Trans. Circuits Syst.* I **43** 817

[21] Parlitz U, Junge L 1996 *Phys. Rev.* E **54** 6 253

[22] Dedieu H, Ogorzalek M J 1997 *IEEE Trans. Circuits Syst.* I **44** 948

[23] Maybhate A, Amritkar R E 1999 *Phys. Rev.* E **59** 284

[24] Hu G L, Feng Z J, Meng R L 2003 *IEEE Trans. Circuits Syst.* I **50** 275

Hop-parameter chaotic synchronization and its applications

Zhang Yong[1)2)] Chen Tian-Qi[1)] Chen Bin[1)]

1)(*School of Electronic Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 610054, *China*)

2)(*School of Electronics*, *Jiangxi University of Finance and Economics*, *Nanchang* 330013, *China*)

(Received 14 March 2006; revised manuscript received 15 May 2006)

Abstract

In this paper, we build a mathematic model of hop-parameter chaotic synchronization, propose and prove its sufficient condition, then analyze theoretically the condition for its realization. An efficient algorithm is proposed for about the hop-parameter chaotic synchronization and hop-parameter period synchronization. Based on the Chua's system, we have simulated the hop-parameter chaotic synchronization and its secure communication. Finally, the counteraction between the hop-parameter chaotic communication system and the wiretapping system is discussed. The simulation shows the hop-parameter chaotic synchronization and its secure communication have the virtue of easy realization and good security.

Keywords: chaotic synchronization, hopped parameter, sufficient condition, secure communication

PACC: 0545