第 54 卷 第 11 期 2005 年 11 月
1000-3290/2005/54(11)/5039-09

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.11,November,2005

混沌同步的充分条件及应用

陈 滨 刘光祜 张 勇 周正欧

(电子科技大学电子工程学院,成都 610054)

(2005 年 2 月 4 日收到;2005 年 4 月 10 日收到修改稿)

对两大类常用连续混沌系统,给出了同步的充分条件,以及状态变量的演化范围,对其作了证明,从理论上分析了这些充分条件一定可实现. 作为应用,证明了时变参数混沌同步的实现充分条件,并用 Chua 系统仿真实现. 时变参数混沌同步通信具有强抗破译性,也给出其抗破译的仿真.

关键词:条件 Lyapunov 指数(CLE),Chua 电路,参数同步

PACC:0545

1. 引 言

近来,利用混沌系统的同步信号作为载波进行保密通信,受到学术界的广泛关注[1—14]. 但其理论上还不完善,给应用带来很多不便.

隐式的混沌同步条件,由文献[2,3]给出必要条件,即响应子系统条件 Lyapunov 指数(CLE)小于 0. 之所以是必要条件,文献[2,3]没有给出状态变量的初值及演化的值对同步的影响. 大量文献在用到隐式的混沌同步条件时,仅提到满足必要条件,避开初值及演化过程取值的问题. 这在很大程度限制了混沌同步的运用,复杂的混沌组合系统,往往牵涉到初值及演化值的影响.

分块线性混沌系统、二阶可微混沌系统,这两类混沌系统几乎囊括目前常用的混沌系统. 本文对此二类混沌系统,给出了同步的充分条件,以及状态变量的演化范围,并对其作了严格证明,并证明了此条件一定可实现.

作为上述充分条件的应用,文中证明了时变参数混沌同步的实现充分条件,并用 Chua 系统作了仿真实现. 时变参数混沌同步具有强抗破译性,当前各种混沌破译方法[15—23]均对其无效. 其抗破译的仿真,也在文中给出.

2. 两大类混沌系统同步的充分条件及其状态变量的演化范围

引用定义 设 $A\in R^{n\times n}$,若对任何非零向量 $X\in R^n$,都有 $X^{\mathrm{T}}AX>0$,则称 A 为广义正定矩阵.

文中提到的广义正定矩阵均为此定义.

一般的 M 维连续混沌同步系统为时不变非线性系统,可以表示为

驱动系统

$$\frac{\mathrm{d}X_0(t)}{\mathrm{d}t}=f(X_0(t)), \tag{1}$$

响应系统

$$\frac{\mathrm{d}X_0'(t)}{\mathrm{d}t}=f(X_0'(t))+QW(X_0(t)-X_0'(t)), \tag{2}$$

式中,状态变量 $X_0(t)\in R^M$,$X_0'(t)\in R^M$. $Q\in R^{M\times M}$,$W\in R^{M\times M}$,Q,W 都为常数矩阵.

响应子系统的雅可比矩阵为

$$J_R(X_0'(t))=\frac{\mathrm{d}\left(\frac{\mathrm{d}X_0'(t)}{\mathrm{d}t}\right)}{\mathrm{d}X_0'(t)}=\frac{\mathrm{d}f(X_0'(t))}{\mathrm{d}X_0'(t)}-QW, \tag{3}$$

式中 $\mathrm{d}f(X_0'(t))/\mathrm{d}X_0'(t)\in R^{M\times M}$,为 $f(X_0'(t))$ 的雅可比矩阵,$J_R(X_0'(t))\in R^{M\times M}$.

做如下约定 对于(1)式的混沌驱动系统,由初始点开始演化,还未演化到混沌吸引子的状态称为混沌过渡态. 在混沌吸引子范围内演化的状态称为混沌态. 文中提到的距离均为欧氏距离.

(1)式的混沌驱动系统,当初值 $X_0(t)$ 在一定范围内,可以演化到混沌态,此范围称为驱动系统的值域 J,显然,驱动系统自由演化中,对任意 $t\in[t_0,+\infty]$,有 $X_0(t)\in J$. (2)式的响应系统,由系统定义所允许的 $X_0'(t)$ 的取值范围,称为响应系统的值域

J',对一般 M 维混沌同步系统,J' 为整个 M 维实空间. 对一般混沌同步系统,有 $J \subset J'$. 文中提到的 J,J' 均为此定义.

混沌系统包括两种常用系统:1) 动力方程的函数 $f(X_0(t))$ 为分块线性函数,且在值域内连续,如 Chua 电路,定义为第一类混沌系统;2) $f(X_0(t))$ 在值域内对 $X_0(t)$ 二阶可微,如 Lorenz 系统,这里定义为第二类混沌系统.

2.1. 第一类混沌系统同步充分条件

第一类混沌系统构成的同步系统为:

驱动系统

$$\frac{\mathrm{d}X_0(t)}{\mathrm{d}t} = A_p X_0(t), \tag{4}$$

响应系统

$$\frac{\mathrm{d}X'_0(t)}{\mathrm{d}t} = A_p X'_0(t) + QW(X_0(t) - X'_0(t)), \tag{5}$$

其中,驱动系统值域 J 被划分成 P_0 块,每块编号为 p,有

$$J = \bigcup_{p=1}^{P_0} J_p,$$

对任意 $p_1 \neq p_2$,有

$$J_{p_1} \cap J_{p_2} = \Phi.$$

显然,响应系统的 J' 也被划分为同样的 P_0 块. $A_p \in R^{M\times M}$,$p = 1,2,\cdots,P_0$,在每块内,A_p 为常数矩阵,定义 A_p 为同步系统的状态变量矩阵. 在值域内,包括分块边界上有 $A_p X_0(t)$ 连续. $Q \in R^{M\times M}$,$W \in R^{M\times M}$ 都为常数矩阵.

定理 1 由(4)式和(5)式定义的混沌同步系统,若初值 $X_0(t_0) \in J$,$X'_0(t_0) \in J'$,且演化过程中有 $X_0(t) \in J$,$X'_0(t) \in J'$,连线 $X_0(t)X'_0(t) \in J'$. 若存在正定实对角矩阵 $D \in \mathrm{diag}(\lambda_1,\cdots,\lambda_M)$,对全部 A_p,以及 $X'_0(t) \in J'$,均有 $D^2(-J_R(X'_0(t)))$ 为广义正定矩阵,其中 $J_R(X'_0(t))$ 为(3)式定义的响应子系统雅可比矩阵. 令 $Y_0(t) = DX_0(t)$,$Y'_0(t) = DX'_0(t)$,误差系统 $S_{0Y}(t) = (Y_0(t) - Y'_0(t))$,$S_{0X}(t) = (X_0(t) - X'_0(t))$. 则有,系统 $S_{0Y}(t)$ 及 $S_{0X}(t)$ 的零解是一致渐进稳定的,且演化过程中有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

证明

$$\frac{\mathrm{d}S_{0Y}(t)}{\mathrm{d}t} = D(A_p - QW)(X_0(t) - X'_0(t))$$
$$= D(A_p - QW)S_{0X}(t),$$

令 Lyapunov 泛函 $V(t) = S_{0Y}(t)^{\mathrm{T}} S_{0Y}(t) = |S_{0Y}(t)|^2$,有 $V(t)$ 正定. 分以下三种情况证明 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定,这三种情况包含了演化中所有可能的情况:

1) 当时刻 t,$X_0(t)$ 与 $X'_0(t)$ 在同一个分块值域内,设分块值域编号为 p,有

$$J_R(X'_0(t)) = -(QW - A_p),$$
$$\frac{\mathrm{d}V(t)}{\mathrm{d}t} = -(S_{0X}(t))^{\mathrm{T}}((D^2(QW - A_p))^{\mathrm{T}} + (D^2(QW - A_p)))(S_{0X}(t)).$$

由 $D^2(-J_R(X'_0(t)))$ 广义正定,可得 $\mathrm{d}V(t)/\mathrm{d}t$ 和 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

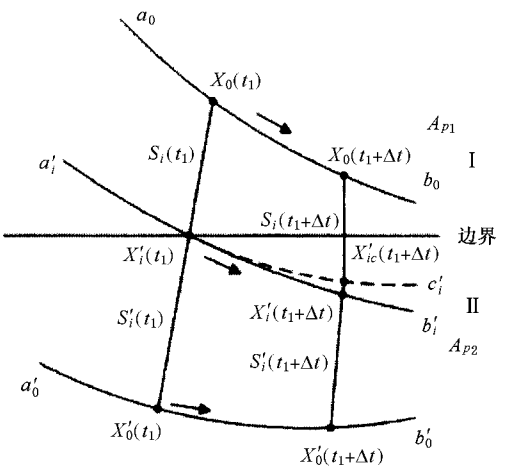

图 1 $X_0(t_1)$ 与 $X'_0(t_1)$ 在二相邻分块值域内

2) 当 $X_0(t_1)$ 与 $X'_0(t_1)$ 在两个相邻分块值域的任意时刻 t_1,图 1 为示意图,边界上面为 I 区,状态变量矩阵为 A_{p1};下面为 II 区,矩阵为 A_{p2},曲线 $a_0X_0(t_1)b_0$ 为驱动系统(4)过 $X_0(t_1)$ 的轨迹,$a'_0X'_0(t_1)b'_0$ 为响应系统(5)过 $X'_0(t_1)$ 的轨迹. 连线 $X_0(t_1)X'_0(t_1)$ 与边界的交点为 $X'_i(t_1)$,作两条辅助曲线 $a'_iX'_i(t_1)b'_i$ 和 $a'_iX'_i(t_1)c'_i$,其中 $a'_iX'_i(t_1)b'_i$ 为响应系统(5)式过 $X'_i(t_1)$ 的演化轨迹;$a'_iX'_i(t_1)c'_i$ 为动力系统(6)式过 $X'_i(t_1)$ 的演化轨迹.

$$\frac{\mathrm{d}X'_{ic}(t)}{\mathrm{d}t} = A_{p1}X'_{ic}(t) + QW(X_0(t) - X'_{ic}(t)), \tag{6}$$

式中,在 I,II 区的状态变量矩阵均为 A_{p1}.

令在时刻 t_1,$S_{iY}(t) = D(X_0(t) - X'_{ic}(t))$,$S'_{iY}(t) = D(X'_0(t) - X'_i(t))$.

同理可得 $\left.\frac{\mathrm{d}|S_{iY}(t)|}{\mathrm{d}t}\right|_{t=t_1}$,$\left.\frac{\mathrm{d}|S'_{iY}(t)|}{\mathrm{d}t}\right|_{t=t_1}$ 负定.

注意到 $\left.\frac{\mathrm{d}X'_{ic}(t)}{\mathrm{d}t}\right|_{t=t_1} = \left.\frac{\mathrm{d}X'_i(t)}{\mathrm{d}t}\right|_{t=t_1}$，可得

$$\left.\frac{\mathrm{d}(|S_{iY}(t)| + |D(X'_{ic}(t) - X'_i(t))| + |S'_{iY}(t)|)}{\mathrm{d}t}\right|_{t=t_1}$$

$$= \left.\frac{\mathrm{d}|S_{0Y}(t)|}{\mathrm{d}t}\right|_{t=t_1}$$ 负定.

3)当 $X_0(t)$ 与 $X'_0(t)$ 在不相邻的分块值域内时，用类似方法可得 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定. 当 $X_0(t)$ 与 $X'_0(t)$ 在边界上，因为它们的导数连续，同样可证得 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

综上可以得出，演化过程中，有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定，所以 $\mathrm{d}V(t)/\mathrm{d}t$ 负定.

$X_0(t) \in J$ 有界. 在初值选定时，$X'_0(t_0)$ 也有界，又因为 $|S_{0Y}(t)|$ 单调减小，所以 $X'_0(t)$ 有界，又因 D, A_p, QW 均范数有界，所以误差系统 $\mathrm{d}S_{0X}(t)/\mathrm{d}t$ 及 $\mathrm{d}S_{0Y}(t)/\mathrm{d}t$ 范数有界.

同步系统(4)，(5)的方程左边均不含 t，是时不变系统.

综上，由 Lyapunov 稳定性理论，$S_{0Y}(t)$ 及 $S_{0X}(t)$ 零解一致渐进稳定，且演化中 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

2.2. 第二类混沌系统同步充分条件

第二类混沌系统构成的同步系统为

驱动系统

$$\frac{\mathrm{d}X_0(t)}{\mathrm{d}t} = f(X_0(t)), \tag{7}$$

响应系统

$$\frac{\mathrm{d}X'_0(t)}{\mathrm{d}t} = f(X'_0(t)) + QW(X_0(t) - X'_0(t)), \tag{8}$$

式中，状态变量 $X_0(t) \in R^M$，$X'_0(t) \in R^M$，$f(X_0(t))$ 值域内对 $X_0(t)$ 二阶可微.

定理 2　由(7)式和(8)式定义的混沌同步系统，若 $X_0(t_0) \in J$，$X'_0(t_0) \in J'$. 若存在正定实对角矩阵 $D \in \mathrm{diag}(\lambda_1, \cdots, \lambda_M)$，以及满足 $J \subset J'_D \subset J'$ 的值域 J'_D，当 $X'_0(t) \in J'_D$，有 $D^2(-J_R(X'_0(t)))$ 为广义正定矩阵，其中 $J_R(X'_0(t))$ 为(3)式定义的响应子系统雅可比矩阵. 且演化过程中有 $X_0(t) \in J$，$X'_0(t) \in J'_D$，连线 $X_0(t)X'_0(t) \in J'_D$. 令 $Y_0(t) = DX_0(t)$，$Y'_0(t) = DX'_0(t)$，误差系统 $S_{0Y}(t) = (Y_0(t) - Y'_0(t))$，$S_{0X}(t) = (X_0(t) - X'_0(t))$. 则有，系统 $S_{0Y}(t)$ 及 $S_{0X}(t)$ 的零解是一致渐进稳定的，且演化过程中有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

证明

如图 2 所示，在 t 时刻，驱动系统(7)的状态变量为 $X_0(t)$，响应系统(8)的状态变量为 $X'_0(t)$. 曲线 $a_0X_0(t)b_0$，$a'_0X'_0(t)b'_0$ 分别为驱动系统　响应系统过点 $X_0(t)$，$X'_0(t)$ 的轨迹，$X_0(t)X'_0(t)$ 为 $X_0(t)$，$X'_0(t)$ 间的直线，在 $X_0(t)X'_0(t)$ 上选取点 $\{X'_i(t) \mid i = 1, \cdots, N_0\}$，把 $X_0(t)X'_0(t)$ 分成 (N_0+1) 等份，曲线 $\{a'_iX'_i(t)b'_i \mid i = 1, \cdots, N_0\}$ 为响应系统(8)过点 $\{X'_i(t) \mid i = 1, \cdots, N_0\}$ 的轨迹.

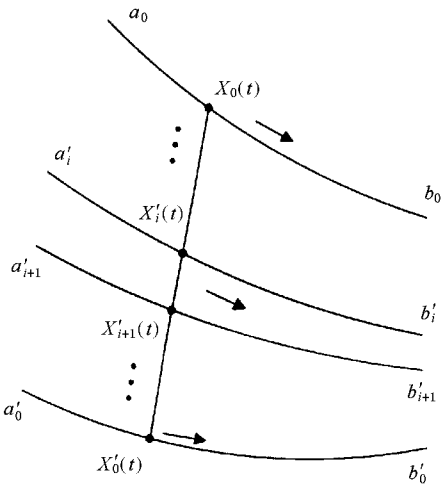

图 2　二阶可微系统演化示意图

令 $S'_{0Y}(t) = D(X_0(t) - X'_1(t)) = Y_0(t) - Y'_1(t)$，

$S'_{iY}(t) = D(X'_i(t) - X'_{i+1}(t)) = Y'_i(t) - Y'_{i+1}(t)$，$i = 1, \cdots, (N_0 - 1)$，

$S'_{N0Y}(t) = D(X'_{N0}(t) - X'_0(t)) = Y'_{N0}(t) - Y'_0(t)$.

当 $N_0 \to +\infty$ 时，$|S'_{iY}(t)| \to 0$，$i = 0, 1, \cdots, N_0$.

下面证明 $\mathrm{d}|S'_{iY}(t)|/\mathrm{d}t$ 负定，$i = 0, 1, \cdots, N_0$.

因为，在 J'_D 内，$f(X_0(t))$ 对 $X_0(t)$ 二阶可微，所以，可以把 $f(X_0(t))$ 在 J'_D 内任一点 $X_0(t_1)$ 作泰勒展开，展开式为

$$f(X_0(t)) = f(X_0(t_1)) + \left.\frac{\mathrm{d}f(X_0(t))}{\mathrm{d}X_0(t)}\right|_{X_0(t)=X_0(t_1)} \times (X_0(t) - X_0(t_1)) + O(|X_0(t) - X_0(t_1)|^2),$$

式中 $O(|X_0(t) - X_0(t_1)|^2)$ 为 $|X_0(t) - X_0(t_1)|$ 的高阶无穷小，当 $|X_0(t) - X_0(t_1)|$ 为无穷小时，有

$$f(X_0(t)) = f(X_0(t_1)) + \left.\frac{\mathrm{d}f(X_0(t))}{\mathrm{d}X_0(t)}\right|_{X_0(t)=X_0(t_1)} \times (X_0(t) - X_0(t_1)).$$

使 $N_0 \to +\infty$，当 $i=0$，$S'_{0Y}(t) = D(X_0(t) - X'_1(t)) = Y_0(t) - Y'_1(t)$，把 $f(X_0(t))$ 在点 $X_0(t)$ 展开，可得

$$\frac{\mathrm{d}\,|\,S'_{0Y}(t)\,|^2}{\mathrm{d}t} = -(X_0(t) - X'_1(t))^{\mathrm{T}}((D^2(-J_R(X'_0(t))))^{\mathrm{T}} + D^2(-J_R(X'_0(t))))(X_0(t) - X'_1(t)).$$

由 $X_0(t)\,X'_0(t) \in J'_D$，$D^2(-J_R(X'_0(t)))$ 广义正定，可得 $\mathrm{d}|S'_{0Y}(t)|/\mathrm{d}t$ 负定.

当 $i=1,2,\cdots,N_0$ 时，同理可得 $\mathrm{d}|S'_{iY}(t)|/\mathrm{d}t$ 负定.

因为

$$|S_{0Y}(t)| = |Y_0(t) - Y'_0(t)| = \sum_{i=0}^{N_0} |S'_{iY}(t)|,$$

所以

$$\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t \text{ 负定}.$$

由于 t 是任取的，且演化过程中有 $X_0(t) \in J$，$X'_0(t) \in J'_D$，连线 $X_0(t)\,X'(t) \in J'_D$，所以在演化过程中均有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

选取 Lyapunov 泛函为 $V(t) = |S_{0Y}(t)|$，有 $V(t)$ 正定，$\mathrm{d}V(t)/\mathrm{d}t$ 负定.

$X_0(t) \in J$ 有界. 初值选定时，$X'_0(t_0)$ 有界，又因 $|S_{0Y}(t)|$ 单调减小，所以 $X'_0(t)$ 有界，因此参数选定时 $f(X_0(t))$，$f(X'_0(t))$ 均范数有界. 又 D，QW 范数有界，所以误差系统 $\mathrm{d}S_{0Y}(t)/\mathrm{d}t$ 和 $\mathrm{d}S_{0X}(t)/\mathrm{d}t$ 范数有界.

系统(7)，(8)是时不变系统.

综上可得，误差系统 $S_{0Y}(t)$ 及 $S_{0X}(t)$ 的零解是一致渐进稳定的，且演化过程中有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定.

2.3. 第一、二类混沌系统同步充分条件及其状态变量演化范围

定理 1 和定理 2 都是假定系统演化中，响应系统状态变量始终满足条件，没确定其演化范围. 这一节通过定理 3 给出状态变量的演化范围.

定义 1 由(1)式定义的 M 维混沌系统，J 为值域，$X_0(t) \in J$. 给定 $D \in \mathrm{diag}(\lambda_1,\cdots,\lambda_M)$ 为正定实对角矩阵，把 J 向外扩展得到 J'_Z，使 $J'_Z = \{Z \mid Z \in R^M, \exists\, X \in J, |D(Z-X)| \leqslant r\}$，其中 $\exists$ 表示存在. r 为正数. 称 J'_Z 为 J 关于 D 的 r 扩展值域. 包含 J'_Z 的最小非凹集，称为非凹扩展值域，记为 $R'_{Dr}(J)$.

定理 3 由(1)和(2)式定义的 M 维混沌同步系统，若其为第一或第二类混沌系统，值域分别为 J，J'. 选定正数 r，若存在正定实对角矩阵 $D \in \mathrm{diag}(\lambda_1,\cdots,\lambda_M)$，当 $X'_0(t) \in R'_{Dr}(J) \subseteq J'$ 时，有 $D^2(-J_R(X'_0(t)))$ 为广义正定矩阵. 且系统初值满足 $X_0(t_0) \in J$，$|D(X_0(t_0) - X'_0(t_0))| \leqslant r$. 令 $Y_0(t) = DX_0(t)$，$Y'_0(t) = DX'_0(t)$，误差系统 $S_{0Y}(t) = (Y_0(t) - Y'_0(t))$，$S_{0X}(t) = (X_0(t) - X'_0(t))$. 则有，系统 $S_{0Y}(t)$ 及 $S_{0X}(t)$ 的零解是一致渐进稳定的，且对任意 $t \in [t_0, +\infty)$，有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定，$X'_0(t) \in R'_{Dr}(J)$. $R'_{Dr}(J)$ 由定义 1 定义.

由定理 1，定理 2 可证得定理 3. 限于篇幅，定理 3 的证明不在此列出.

2.4. 定理 3 的条件可实现性

定理 3 的条件一定可实现.

证明 选取 $QW = \mathrm{diag}(k_1,\cdots,k_M)$ 为正定对角阵，

$$\frac{1}{2}((J_R(X_0(t)))^{\mathrm{T}} + J_R(X_0(t))) = \frac{1}{2}\left(\left(\frac{\mathrm{d}f(X_0(t))}{\mathrm{d}X_0(t)}\right)^{\mathrm{T}} + \frac{\mathrm{d}f(X_0(t))}{\mathrm{d}X_0(t)}\right) - QW,$$

$$\frac{\mathrm{d}f(X_0(t))}{\mathrm{d}X_0(t)} = [a_{ij}],$$

$$a_{ij} \in R, i = 1,2,\cdots,M; j = 1,2,\cdots,M.$$

定理 3 的混沌系统，J 有界. 给定 D 及 r，使 $R'_{Dr}(J) \subset J'$，有 $R'_{Dr}(J)$ 有界，因此 $\mathrm{d}f(X_0(t))/\mathrm{d}X_0(t)$ 的元素有界，即每个 a_{ij} 有界.

当

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

由特征值的圆盘定理可得 $((J_R(X_0(t)))^{\mathrm{T}} + J_R(X_0(t)))/2$ 的每个特征值小于零，因此 $(-J_R(X'_0(t)))$ 广义正定. 所以 $D^2(-J_R(X'_0(t)))$ 也广义正定. 选择初值，使 $X_0(t_0) \in J$，$|D(X_0(t_0) - X'_0(t_0))| \leqslant r$，就可满足定理条件.

综上，定理 3 的条件在理论上一定可实现. 并且，可以通过调整 D 矩阵，使 QW 的元素取较小值时，$D^2(-J_R(X'_0(t)))$ 就广义正定，这样系统比较容易实现.

2.5. 定理 3 用于 Chua 系统的同步实现

Chua 电路的具体电路结构及状态方程见文献[16]. 这里给出文中仿真用到的参数，K_1 为反馈系数，$L = 7.14\text{mH}$，$G_a = -0.8\text{mS}$，$G_b = -0.5\text{mS}$，$E = 1\text{V}$，$R_0 = 5\Omega$，$C_1 = 5\text{nF}$，$C_2 = 68\text{nF}$，$G = 0.68\text{mS}$.

响应系统的值域 J' 为整个 3 维实空间，当 $K_1 = 0.001$，$D = \text{diag}(d_1, d_2, d_3) = \text{diag}(\sqrt{1.25}, \sqrt{13}, \sqrt{1500000})$ 时，对于 $X'_0(t) \in J'$，有 $D^2(-J_R(X'_0(t)))$ 广义正定. 因此，取 r 为任意值，均满足定理 3. 系统的状态向量为 $X_0(t) = (v_1(t), v_2(t), i_3(t))^{\mathrm{T}}$，$X'_0(t) = (v'_1(t), v'_2(t), i'_3(t))^{\mathrm{T}}$. 令 $Y_0(t) = DX_0(t)$，$Y'_0(t) = DX'_0(t)$，误差系统 $S_{0Y}(t) = (Y_0(t) - Y'_0(t)) = (S_{v1}(t), S_{v2}(t), S_{i3}(t))^{\mathrm{T}}$.

仿真结果列于图 3，可见当 $t \in [t_0, +\infty]$，$\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$ 负定，即未同步时，$|S_{0Y}(t)|$ 严格单调减小趋近于零，因此 $X'_0(t) \in R'_{Dr}(J)$，与定理 3 给出的结果一致.

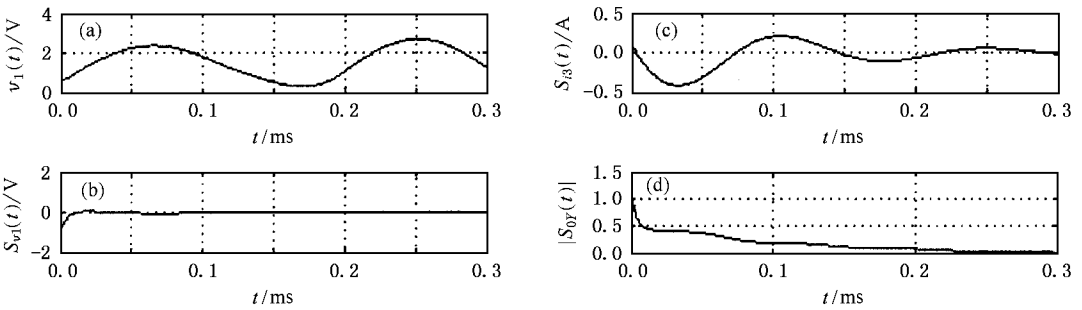

图 3　Chua 系统的混沌同步　(a) 驱动系统状态变量 $v_1(t)$；(b) 误差分量 $S_{v1}(t)$；(c) 误差分量 $S_{i3}(t)$；(d) 误差向量的模 $|S_{0Y}(t)|$

3. 时变参数混沌同步及实现

3.1. 时变参数混沌同步

本文的时变参数混沌同步系统的驱动、响应系统为：

驱动系统

$$\frac{\mathrm{d}X_0(t)}{\mathrm{d}t} = f(X_0(t), \{u_i(t_0 + nT) \mid i = 1, \cdots, H\}). \tag{9}$$

响应系统

$$\frac{\mathrm{d}X'_0(t)}{\mathrm{d}t} = f(X'_0(t), \{u_i(t_0 + nT) \mid i = 1, \cdots, H\}) - QW(X_0(t) - X'_0(t)). \tag{10}$$

当参数固定不变时，系统属于第一或第二类混沌同步系统.

n 为时变参数时钟，时变参数随 n 变化. 虽然 n 很大，但时变参数 $u_i(t_0 + nT) = u'_i(t_0 + nT)$ 的取值可以无规律地重复，不同的取值可较少. 设其共选有 W 组不同取值，分别为 $u_k = u'_k \in R^H$，$k = 1, 2, \cdots, W$.

对任一组参数 $u_k = u'_k$，有：

驱动系统

$$\frac{\mathrm{d}X_0(t)}{\mathrm{d}t} = f(X_0(t), u_k). \tag{11}$$

响应系统

$$\frac{\mathrm{d}X'_0(t)}{\mathrm{d}t} = f(X'_0(t), u'_k) - QW(X_0(t) - X'_0(t)). \tag{12}$$

定义 2　(11)式的混沌驱动系统，对于某组参数 u_k，驱动系统处于的混沌态时的值域，称为驱动系统对于 k 的混沌态值域 $R_{ck}(X_0(t))$. 当驱动系统初值在一定范围内，驱动系统可演化到混沌态，称此范围为驱动系统对 k 的值域 J_k.

显然有 $R_{ck}(X_0(t)) \subset J_k$.

定义 3　对于所有 k，令

$$R_c(X_0(t)) = R_{c1}(X_0(t)) \cup R_{c2}(X_0(t)) \cdots \cup R_{ck}(X_0(t)) \cdots \cup R_{cW}(X_0(t)),$$

$$J_o = J_1 \cap J_2 \cdots \cap J_k \cdots \cap J_W,$$

合理选择参数 u_k，使 $R_c(X_0(t)) \subseteq J_o$，称 $R_c(X_0(t))$ 为驱动系统的混沌态值域.

显然，当 $X_0(t_0) \in R_c(X_0(t)) \subseteq J_o$，驱动系统(11)可以演化到混沌态. 对于所有选定参数 u_k，以

及任意初值 $X_0(t_0)\in R_c(X_0(t))$，存在一个演化到混沌态的所需的最长时间，称为最大过渡时间 T_0，则当 $T\geqslant T_0$ 时，对任意 $X_0(t_0)\in R_c(X_0(t))$，一定有 $X_0(t_0+T)\in R_c(X_0(t))$.

定义 4 (11)式的混沌驱动系统，对某组参数 u_k，对于所有初值 $X_0(t_0)\in R_c(X_0(t))$，$X_0(t)$的演化范围，称为 $X_0(t)$对 k 的限初值值域 $R_k(X_0(t))$. 显然 $R_{ck}(X_0(t))\subseteq R_k(X_0(t))$. 对于所有 k，令

$$R(X_0(t))=R_1(X_0(t))\cup R_2(X_0(t))\cdots\cup R_k(X_0(t))\cdots\cup R_W(X_0(t)),$$

称 $R(X_0(t))$为 $X_0(t)$的限初值值域.

显然有 $R_c(X_0(t))\subseteq R(X_0(t))$.

定义 5 给定 D，r，将 $R(X_0(t))$按定义 1 进行扩展得到 $R'_{Dr}(X'_0(t))$，且 $X'_0(t)$在 $R'_{Dr}(X'_0(t))$内有定义，称其为响应系统(12)式对所有参数 u_k 关于 D 的 r 非凹扩展值域 $R'_{Dr}(X'_0(t))$.

定理 4 对(9)，(10)式定义的时变参数混沌同步系统，若对给定的 D，r，当 $X'_0(t)\in R'_{Dr}(X'_0(t))$，对每组时变参数 u_k，均有 $D^2(-J_R(X'_0(t))$广义正定. 且满足 $X_0(t_0)\in R_c(X_0(t))$，$|D(X_0(t_0)-X'_0(t_0))|\leqslant r$，$T\geqslant T_0$. 令 $Y_0(t)=DX_0(t)$，$Y'_0(t)=DX'_0(t)$，误差系统 $S_{0Y}(t)=(Y_0(t)-Y'_0(t))$，$S_{0X}(t)=(X_0(t)-X'_0(t))$. 则有系统 $S_{0Y}(t)$及 $S_{0X}(t)$的零解是渐进稳定的，且对 $t\in[t_0,+\infty)$，有 $\mathrm{d}|S_{0Y}(t)|/\mathrm{d}t$负定，$X'_0(t)\in R'_{Dr}(X'_0(t))$.

注意到连续动力系统的状态不能跳变(包括在时钟变化处)，可由定理 3 证得定理 4. 限于篇幅，证明不在此列出.

与定理 3 类似，定理 4 条件也是一定可实现的.

3.2. 定理 4 用于 Chua 电路时变参数同步的实现

采用前述的 Chua 电路，$L=7.14\mathrm{mH}$，$G_a=-0.8\mathrm{mS}$，$G_b=-0.5\mathrm{mS}$，$E=1\mathrm{V}$. 时钟周期 $T=100\mu\mathrm{s}$.

驱动、响应系统的时变参数相等，随时钟 n 变化，简记为 $G=G'$，$C_2=C'_2$，$R_0=R'_0$，$C_1=C'_1$. $R_0=R'_0$ 做无规律的 5Ω，10Ω 二值变化，$C_1=C'_1$ 做无规律的 5nF，6nF 二值变化，$G=G'$在[0.63mS，0.68mS]的连续区域内做跳变，$C_2=C'_2$ 在[56nF，68nF]的连续区域内做跳变.

响应系统的值域 J'为整个 3 维实空间，当 $K_1=0.001$，$D=\mathrm{diag}(d_1,d_2,d_3)=\mathrm{diag}(\sqrt{1.25},\sqrt{13},\sqrt{1500000})$时，对上述所有的取值，$D^2(-J_R(X'_0(t))$在 J'内均广义正定. 因此，取 r 为任意值，均满足定理 4 的条件. 令 $Y_0(t)=DX_0(t)$，$Y'_0(t)=DX'_0(t)$，误差系统 $S_{0Y}(t)=(Y_0(t)-Y'_0(t))$. 仿真结果见图 4，当 $t\in[t_0,+\infty]$，有$|S_{0Y}(t)|$单调减小趋近于零，从而 $X'_0(t)\in R'_{Dr}(X'_0(t))$，与定理 4 一致.

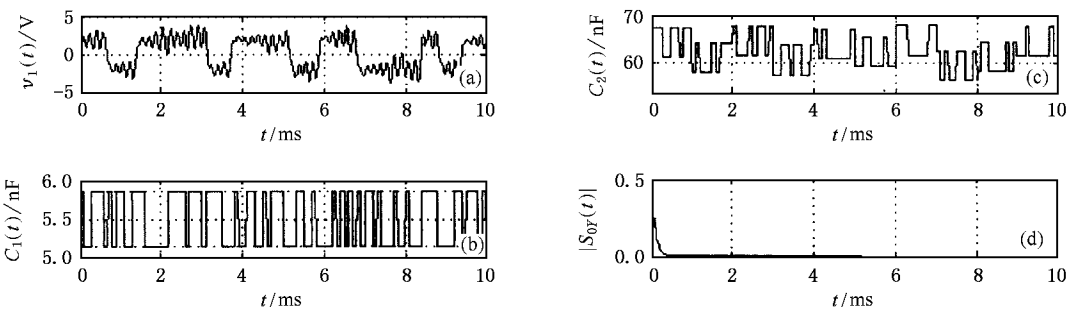

图 4 Chua 混沌同步系统的时变参数同步 (a) 驱动系统状态变量 $v_1(t)$；(b) 时变参数 $C_1(t)=C'_1(t)$；(c) 时变参数 $C_2(t)=C'_2(t)$；(d) 误差向量的模$|S_{0Y}(t)|$

4. 采用时变参数法用参数调制进行混沌同步通信

在上述系统基础上，可以采用混沌掩蔽、混沌开关、混沌调制及混沌键控等多种方式进行混沌同步通信. 本文以 Chua 电路为基础，采用参数调制法进行混沌同步通信[15—18].

选取 G，C_2，R_0 作为时变密钥参数，C_1作为传输信息调制参数. 驱动系统把信号 $I(t)$调制到参数

C_1上，响应系统采用参数自适应算法[15—18]对参数$C_1(t)$进行估计，令响应系统中对$C_1(t)$的估计为$C_1'(t)$，接收方由$C_1'(t)$解调恢复出信息$I(t)$. 仿真证实 Chua 电路的时变参数通信是成功的，限于篇幅，仿真过程及结果不在文中给出.

时变参数作为密钥，应妥善保管. 平时没通信的时候，可以把系统参数设定为非密钥的常态值. 通信的时候，才使用密钥参数，以确保时变参数密钥的保密性.

5. 时变参数混沌同步通信对抗各种窃密攻击

目前破译混沌同步通信的入手点，是针对混沌同步有强烈的参数敏感性，运用广义同步法[20—22]，相图法或变形相图法[19]，参数自适应估计法[15—18]，以及不动点法[23]等等方法破译系统. 由于时变参数对含有信息的参数进行了掩蔽，可以避免系统被这些攻击方法破译.

5.1. 对抗广义同步方法的攻击

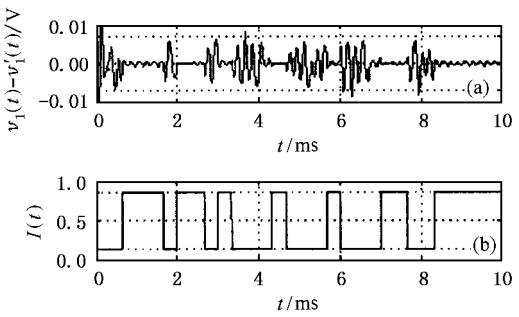

图 5　广义同步法对一般混沌同步通信的攻击　(a)驱动信号与响应信号之差 $v_1(t)-v_1'(t)$；(b) 传输的信号 $I(t)$

广义同步攻击[20—22]，是窃密者使用自制响应系统(结构可以与驱动系统不同)，与驱动系统形成广义同步，从而破译出所含信息. 图 5 表示未采用时变参数进行通信，窃密者可以通过同步误差的幅度窃取到所需信息；图 6 表示采用时变密钥参数进行通信，窃密者无法窃取到所需信息.

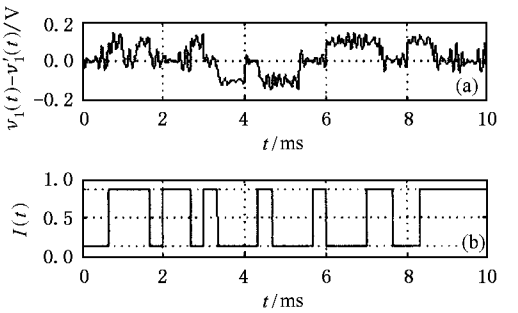

图 6　广义同步法对时变密钥参数混沌同步通信的攻击　(a)驱动信号与响应信号之差 $v_1(t)-v_1'(t)$；(b) 传输的信号 $I(t)$

5.2. 对抗相图及变形相图法的攻击

相图法或变形相图法的攻击[19]，是利用含有不同信息的混沌信号，在相图或变形相图(比如回归影射相图)上，呈现出不同的位置及特点，通过度量这些差异，破译出所需的信息. 由于时变参数混沌同步通信的传输信息$I(t)$被时变参数掩蔽，在相图上无法正确度量差异而破译信息.

图 7，图 8 所示仿真采用文献[19]的方法进行攻击. 定义M_n为$v_1(t)$的第n个极大值，I_n为$v_1(t)$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 VS B_n和$-C_n$ VS $-D_n$画在同一张相图上就得到图 7 和图 8 所示的相图.

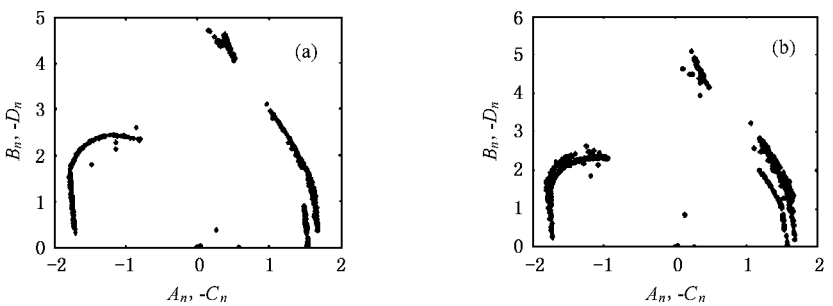

图 7　回归相图法攻击一般混沌同步通信　(a) $I(t)=0$ 的基准相图；(b) $I(t)$为 0，1 二值信息的相图

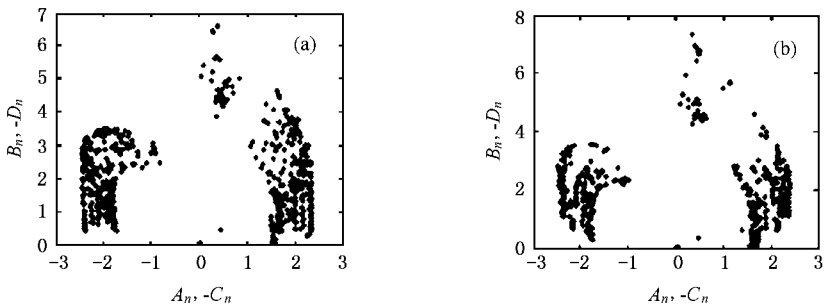

图 8 回归相图法攻击时变参数混沌同步通信 (a) $I(t)=0$ 的基准相图；(b) $I(t)$ 为 0,1 二值信息的相图

从图 7 可知，一般混沌同步通信，不含信息(或只含信息 0)的基准相图较清晰，含信息的相图与之相比有明显区别，对比其异同，窃密者可得知信息. 而从图 8 可知，时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区域，无法作为基准，窃密者无法得知有用信息.

5.3. 对抗参数自适应估计法的攻击

参数自适应估计法的攻击[15—18]，是窃密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信号的参数，从而破解出所需信息. 由于窃密者未知的参数比通信方多得多，在时钟周期 T 内，通信方可估计出信息参数，而窃密方则无法估计出所需参数. 由图 9 和图 10 可知，用参数自适应算法窃密，未采用时变参数的混沌同步通信被破解，采用时变参数则无法被破解.

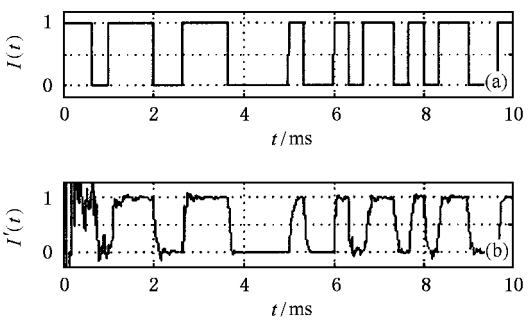

图 9 参数自适应估计法对一般混沌同步通信的攻击 (a) 传输的信号 $I(t)$；(b) 窃密方恢复出的信号 $I'(t)$

5.4. 对抗不动点法的攻击

不动点法的攻击[23]，要求窃密者知道通信系统结构，并进入通信系统内部，在接收系统的输入端输入常数，接收方混沌系统的状态变量会收敛到常数，

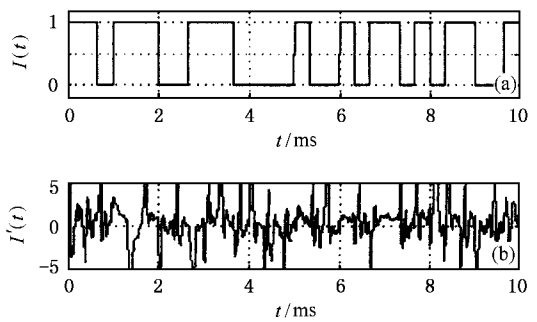

图 10 参数自适应估计法攻击时变参数混沌同步通信 (a) 传输的信号 $I(t)$；(b) 窃密方恢复出的信号 $I'(t)$

根据输入的常数以及对应的状态变量的常数值，解出系统参数，这对窃密者的要求很高. 此方法对时变参数混沌同步通信系统无效，正确保管密钥的前提下，平时系统的参数是非密钥的常态值，这时窃密者只能得到这些常态值，正式通信时参数已发生变化，且呈时变状态，这些常态参数对破译信息没有帮助.

5.5. 讨 论

Chua 系统是一种只有一个正的 LE 指数的混沌系统，抗破译性不高；参数调制的混沌同步通信也是一种简单调制通信方法，抗破译性低. 但与时变参数混沌同步通信结合，具有了很高的抗破译性，说明此方法抗破译性很好.

6. 结 论

本文对分块线性混沌系统，二阶可微混沌系统这两大类常用混沌系统，给出了同步的充分条件及状态变量的演化范围，对其作了证明，并证明了这些充分条件一定可实现. 作为应用，证明了时变参数

混沌同步的实现充分条件，并用 Chua 系统仿真，仿真结果同理论一致. 此方法用于保密通信具有极高的保密性，可以击败目前的各种破译方法的攻击，其击败各种窃密攻击的仿真证实了其高保密性.

[1] Carrol T L 2002 *IEEE Trans. Curcuits. Syst.* I **49** 357

[2] Pecora L M and Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[3] Carroll T L and Pecora L M 1991 *IEEE Trans. Circuits Syst.* **38** 453

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

[5] Pastur L, Boccaletti S and Ramazza P L 2004 *Phys Rev.* E **69** 036201

[6] Liu F C, Wang J and 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]

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

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

[9] Luo X S, Fang J Q, Wang L H *et al* 1999 *Acta Phys. Sin.* **48** 2022(in Chinese) [罗晓曙、方锦清、王力虎 等 1999 物理学报 **48** 2022]

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

[11] Bragard J, Boccaletti S and Arecchi F T 2001 *Int. J. Bifurcation and Chaos* **11** 2715

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

[13] Zhou C S and Lai C H 1999 *Phys Rev.* E **60** 320

[14] Zhan M, Wang X G and Gong X F 2003 *Phys Rev.* E **68** 036208

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

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

[17] Parlitz U and Junge L 1996 *Phys Rev.* E **54** 6 253

[18] Maybhate A and Amritkar R E 1999 *Phys Rev.* E **59** 284

[19] Perez G 1995 *Phys Rev. Lett.* **74** 6 253

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

[21] Kocarev L and Parliz U 1996 *Phys Rev. Lett.* **76** 1 816

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

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

Sufficient conditions of chaotic synchronization and its applications

Chen Bin　Liu Guang-Hu　Zhang Yong　Zhou Zheng-Ou

(*School of Electronic Engineering, UEST of China, Chengdu* 610054, *China*)

(Received 4 February 2005; revised manuscript received 10 April 2005)

Abstract

At present time, only necessary conditions of chaotic synchronization are known, and applications of chaotic synchronization is limited. In this paper, sufficient conditions of continuous chaotic system synchronization and the proofs are presented, and evolutive range of state variables is presented, too. We proved the conditions are realizable. As an application of the theory, we proved sufficient conditions of time-varying parameter chaotic synchronization, and made simulations by Chua circuits. Time varying parameter chaotic synchronization communication has high security performance, and the simulations that it defeat all kinds of attacks of eavesdroppers are presented.

Keywords: conditioned Lyapunov exponents (CLE), Chua circuit, parameter synchronization

PACC: 0545