カオス同期化制御とその秘匿通信への応用

潮 俊光†

2個のサブシステムの振る舞いはカオス的であるが，各時刻での状態が等しくなるような現象はカオス同期と呼ばれる．本論文では，離散時間非線形システムがカオス同期化するような制御手法を提案する．カオス同期化制御法として有名なLaiとGrebogiの方法では，カオス軌道のまわりでの線形化時変システムを基に制御器が構成されるため，システムが微分可能であるという仮定が必要である．本手法では，縮小写像の性質を利用するので，システムの微分可能性を仮定する必要はなく，さらに，制御器の構成もかなり簡単になる．次に，本手法を秘匿通信システムの構成に応用する．各サブシステムは同期化部，変調部，復調部からなり，送信信号の内容は情報信号の送信方向によって決定される．既に，カオス同期化を利用した秘匿通信法は提案されているが，すべてが単方向通信である．本手法を用いると，駆動システムを変更できるので，半二重通信が可能となる．最後に，カオスシステムとしてエノン写像を用いた通信システムを例に取り，本通信法の有効性を示す．

Chaotically Synchronizing Control and Its Application to Secure Communication

TOSHIMITSU USHIO †

Chaotic synchronization is a nonlinear phenomenon such that two subsystems are chaotic but their states take same values at each time. This paper proposes a control method for synchronizing discrete-time nonlinear systems chaotically. Lai and Grebogi's method is a very famous control method for chaotic synchronization. Their method requires the differentiability of controlled systems because it is based upon a time-varying linearized system around chaotic behaviors. The proposed method is based upon a property of contraction mappings. So it can apply to nondifferentiable systems, and the design procedure is simpler than Lai and Grebogi's method. Next, we propose a secure communication system using the proposed method. Each subsystem consists of a synchronization device, a modulation device and a demodulation device. And transmitted signals are determined according to which way an informational signal is transmitted. Many secure communication systems based upon chaotic synchronization are simplex. But the proposed system is half-duplex because a driving subsystem can be changed by control. Finally, we illustrate a secure communication system whose synchronization device is described by the Hénon mapping.

1. はじめに

カオス同期とは，二つのサブシステムの振る舞いはともにカオス的振動であるが，各時刻での状態が等しくなる現象である[1]．カオス同期化法を最初に提案したのは，PecoraとCarroll[1]である．彼らは，システムSを二つの部分システムS_1, S_2に分け，S_2と全く同じシステムS_2'を新たに構成し，S_2'へS_1の状態を入力すると，ある条件の下で，S_2とS_2'の状態が同期することを示した．この手法を用いたChua回路におけるカオス同期化が報告されている[2]．さらに，カスケード結合をした非線形ネットワークへの拡張が提案されている[3]．

PecoraとCarrollの方法はカオス同期するようなシステムの構成法なので，構成されたシステムにおいては常にカオス同期が達成される．そのため必要なときだけカオス同期させることはできない．この問題を解決するためには，カオス同期を行いたいときに何らかの制御を施して，カオス同期を達成することが必要となる．カオスの制御において有名な方法に，Ott, Grebogi, YorkeによってOGY法がある[4]．Mehtaら[5]，Laiら[6]は，OGY法を修正して，カオス同期化のための制御法を提案した．例えば，LaiとGrebogiの方法[6]では，動特性が同じ二つのサブシステムを考えているが，そのサブシステムの状態が他方

† 大阪大学工学部電子工学科
Department of Electronic Engineering, Osaka University

へ干渉しないと仮定されている．すなわち，制御をしなければ，この二つのサブシステムは全く独立に振る舞うことになる．制御入力は一方のサブシステムのみに施される．したがって，制御入力がないサブシステムの振る舞いに，制御入力のあるサブシステムが追従するような同期化になっている．このとき，制御入力のないサブシステムは駆動システムと呼ばれる．筆者は，大規模システムにおいて，複数個のサブシステムの状態を同期化させるようなフィードバックの構成法を提案している[7)~9)]．さらに，カオスニューラルネットワークにおけるカオス同期化制御についても考察している[10),11)]

カオス同期の伝送システムへの応用については既に多くの研究がある[12)~15)]．しかしながら，そのほとんどがChua回路などのアナログ回路を用いている．ディジタル通信が普及した現在では，ディジタル信号の秘匿化が重要である．そのためには，離散時間システムのカオスを利用することになる[16)]．ところで，既に，シフトレジスタ等を用いて作成された疑似乱数列とバイナリ信号を混合させるスクランブル法が研究されている[17),18)]．カオス同期を用いる場合には，バイナリ信号に変換する前に信号を秘匿化することになり，この点がスクランブル法とは異なる．

ここでは，サブシステム間に相互干渉がある離散時間システムに対するカオス同期化制御法を提案し，その方法をディジタル信号の秘匿通信に応用する．まず，2章で，状態フィードバックによるカオス同期化制御法を提案する．本手法の適用できるクラスは，LaiとGrebogiの方法でカオス同期化できるシステムのクラスを含んでいる．LaiとGrebogiの方法は，同期化された振る舞いのまわりでの線形化時変システムを用いてフィードバックゲインを計算しているが，本手法では，このような計算をせずに簡単に制御入力が求められる．3章で，2章で提案したカオス同期化制御法を用いた秘匿通信法を提案する．従来のカオスを利用した通信法は1方向の通信法であったが，ここでは，半2重の通信法となる．4章では，エノン写像を用いた秘匿通信システムの例を用いて，本通信法の有効性を調べる．

以下，本論文では，写像 h_1 と h_1 に対して，h_1+h_2 および $h_1\circ h_2$ を以下のように定義する．

$$(h_1+h_2)(x):=h_1(x)+h_2(x)$$
$$(h_1\circ h_2)(x):=h_1(h_2(x))$$

2. 同期化制御

ここでは，同じ動特性をもつ2個のサブシステム S_1，S_2 からなる離散時間非線形システムを考える．各サブシステムは次の差分方程式で記述される．

$$x_i(k+1)=f(x_i(k))+g(x_1(k),x_2(k))+bu_i(k)\qquad i=1,2 \qquad (1)$$

ただし，$x_i(k)\in R^n$ はサブシステム S_i の状態（n はシステムの次元），$u_i(k)\in R^l$ は S_i の入力（l は入力数），$b\in R^n\times^l$ は定数行列，$f:R^n\to R^n$ は各サブシステムの動特性を，$g:R^{2n}\to R^n$ はサブシステム間の干渉を表す．式（1）に制御入力がないとき，すなわち $u_i(k)\equiv 0$ $(i=1,2)$ のとき，カオスになっていると仮定する．

次に，$x_1(k)$ と $x_2(k)$ が同期するような制御を提案する．今，サブシステム S_1 を駆動システムと考え，S_2 が S_1 の振る舞いに追従するような制御を考える．そこで，$x_1(k)$ と $x_2(k)$ の重み付けされた差 $D(k)$ を次のように定義する．

$$D(k):=h(x_2(k))-h(x_1(k))$$

ただし，h は R^n から R^l への写像である．状態 $x_1(k)$ と $x_2(k)$ が同期しているときには，$D(k)=0$ となる．ここで，制御入力としてこの差を用いた，次の状態フィードバックを考える．

$$u_1(k)=0$$
$$u_2(k)=KD(k)=K(h(x_2(k))-h(x_1(k))) \qquad (2)$$

ただし，$K\in R^{l\times l}$ はフィードバックゲインを表す．同期が達成されたときに制御入力は0となり，経済的な制御といえる．また，このことより，その同期した振る舞いが収束するカオスアトラクタは，制御されていないシステムにおいてはカオス集合になっている．すなわち，式（2）は，システムに存在するカオス同期に対応するカオス集合をアトラクタにするような制御になっている．以下に式（2）により同期化できるための十分条件を示す．

【命題1】 写像 $h:R^n\to R^l$ とゲイン $K\in R^{l\times l}$ は次の条件を満足すると仮定する．

C1： 任意の $x,y\in R^n$ に対して，次式を満たす $\alpha(0\le\alpha<1)$ が存在する．

$$\|(f+bKh)(x)-(f+bKh)(y)\|\le\alpha\|x-y\| \qquad (3)$$

このとき，式（2）によって式（1）は同期化される．すなわち，

$$\lim_{k\to\infty}\|x_1(k)-x_2(k)\|=0 \qquad (4)$$

となる．

（証明） 式（1），（2）および条件C1より

$$\|x_1(k+1)-x_2(k+1)\|$$
$$=\|(f+bKh)(x_1(k))-(f+bKh)(x_2(k))\|$$
$$\le\alpha\|x_1(k)-x_2(k)\|$$

したがって，$0\le\alpha<1$ なので，式（4）が成立する．■

ところで，証明から明らかなように，システムがカオス的であるときには，状態は有界なので，以下の条件が成立すれば $x_1(k)$ と $x_2(k)$ はカオス同期化される．

C1′： 十分大きな領域 $\mathcal{R}\subset R^n$ において，任意の $x, y\in\mathcal{R}$ に対して式（3）が成立するような α $(0\leq\alpha<1)$ が存在する．

カオスの制御において最も有名な方法である OGY 法の特徴の一つに，小さな制御入力で目標の軌道を安定化できる点がある．本手法においても，同期化に対応するカオス集合が制御入力のないシステムにおけるカオスアトラクタの中に埋め込まれている場合には，次のように式（2）の $u_2(k)$ を変更することにより，条件 C 1′が満足されるならば，小さな制御入力で同期化が達成できる．

$$u_2(k)=\begin{cases}KD(k) & \text{if } \|D(k)\|<\varepsilon\\ 0 & \text{otherwise}\end{cases}$$

ところで，式（2）は，h が線形で，$g(x_1, x_2)\equiv 0$ のとき Lai と Grebogi の方法[6]を含むことになるが，その設計手順は全く異なる．Lai と Grebogi の方法では，同期化される振る舞いのまわりでの線形化時変システムに基づいてゲインが計算される．そのために，f が微分可能であることが要求される．しかし，本手法では，f が微分不可能であっても条件 C 1 または C 1′を満足するならば同期化が達成できる．さらに，ヤコビ行列を求めなくてよいので，そのフィードバックの設計もかなり簡単になる．

3. 秘匿通信システム

前章で提案した同期化制御を適用した半 2 重秘匿通信システムを提案する．サブシステム S_1 と S_2 の間で通信を行う．各サブシステムは，同期化部，変調部，復調部からなる．各部は次式で表される．

- 同期化部：
$$x_i(k+1)=f(x_i(k))+bu_i(k) \qquad (5)$$
- 変調部：
$$w_i(k+1)=p(x_i(k), w_i(k), s_i(k+1)) \qquad (6)$$
- 復調部：
$$t_i(k+1)=p^{-1}(x_i(k-1), v_i(k-1), v_i(k)) \qquad (7)$$

ただし，$x_i(k)\in R^n$，$w_i(k)\in R$ および $t_i(k)\in R$ はそれぞれ同期化部，変調部，復調部の状態，$u_i(k)\in R$ と $v_i(k)\in R$ は制御入力，$s_i(k)$ は情報信号，$b\in R^n$ は定数ベクトルを表す．写像 $f:R^n\to R^n$ はカオス的であると仮定し，写像 $p:R^n\times R\times R\to R$ は以下の条件を満足すると仮定する．

- 任意の $x\in R^n$ と $w\in R$ に対して，$p(x, w, \cdot)$ には逆写像が存在する．この逆写像を $p^{-1}(x, w, \cdot)$ と書く．

また，S_1 から S_2 および S_2 から S_1 へ送信される信号をそれぞれ $c_{12}(k), c_{21}(k)$ とおく．これらの送信信号から直接情報信号 $s_i(k)$ が復元できないようにする必要がある．そのために，$w_i(k)$ が $x_i(k)$ と異なるカオス的振る舞いをするように写像 g を選ぶことが重要である．

制御入力 $u_i(k)$, $v_i(k)$ および送信信号 $c_{12}(k), c_{21}(k)$ としてどのような信号をセットするかは，情報信号を送信する方向に依存する．ここでは，S_1 から S_2 へ情報信号を送る場合を考える．このとき，以下のように信号をセットする．

$$\left.\begin{aligned}&c_{12}(k)=m_{12}(w_1(k))\\&c_{21}(k)=m_{21}(x_2(k))\\&u_1(k)=h(m_{21}(x_1(k)))-h(c_{21}(k))\\&u_2(k)=0\\&v_1(k)=0\\&v_2(k)=m_{12}^{-1}(c_{12}(k))\end{aligned}\right\} \qquad (8)$$

ただし，$m_{12}:R\to R$ は 1 対 1 写像で，写像 $h:R\to R$ と $m_{21}:R^n\to R$ は以下の条件を満足している．

C2： 任意の $x, y\in R^n$ に対して次式を満たすような α $(0\leq\alpha<1)$ が存在する．

$$\|(f+bh\circ m_{12})(x)-(f+bh\circ m_{12})(y)\|\leq\alpha\|x-y\|$$

命題 1 と条件 C 2 より，

$$\lim_{k\to\infty}\|x_1(k)-x_2(k)\|=0$$

が得られる．ここで，

$$s_1(k+1)=p^{-1}(x_1(k), w_1(k), w_1(k+1))$$

なので，

$$\lim_{k\to\infty}|t_2(k+1)-s_1(k)|=0$$

となる．すなわち，情報信号 $s_1(k)$ は S_2 において $t_2(k+1)$ として復元されることが分かる．同様にして，S_2 から S_1 へ情報信号 $s_2(k)$ を伝送することができる．従って，この伝送法により半 2 重通信が可能となる．カオスを利用した秘匿通信法は多く提案されてきたが[12)~16)]，いずれもが単信方式である．本手法では，カオスの同期化制御を利用することにより，駆動システムを変更できるという特徴を利用しているので，半 2 重通信が可能となる．

4. 例　　題

ここでは，同期化部としてエノン写像を用いた以下のような通信システムを考える．

- 同期化部：

$$x_i(k+1)=1.4-x_i^2(k)+y_i(k)+u_i(k)$$
$$y_i(k+1)=0.3x_i(k)$$

- 変調部：

$$w_i(k+1)=|9y_i(k)w_i(k)(1-w_i(k))|+(|4w_i(k)(1-w_i(k))|+0.1)(0.1|y_i(k)|+s_i(k+1))$$

- 復調部：

$$t_i(k+1)=\frac{v_i(k)-|9y_i(k-1)v_i(k-1)(1-v_i(k-1))|}{|4v_i(k-1)(1-v_i(k-1))|+0.1}-0.1|y_i(k-1)|$$

情報信号 $s_1(k)$ を S_1 から S_2 へ伝送することを考える．制御入力および伝送信号を以下のようにセットする．

$$c_{12}(k)=w_1(k)$$
$$c_{21}(k)=x_2^2(k)-0.5y_2(k)$$
$$u_1(k)=x_1^2(k)-0.5y_1(k)-c_{21}(k)$$
$$u_2(k)=0$$
$$v_1(k)=0$$
$$v_2(k)=c_{12}(k)$$

このとき，条件C2が成立することが容易に示される．したがって，$t_2(k)$ は $s_1(k-1)$ に収束する．以下，情報信号として，

$$s_1(k)=0.01\sin(0.1k) \qquad (9)$$

を与えた場合を考える．**図1**に復調信号 $t_2(k)$ およびその情報信号との差 $t_2(k)-s_1(k-1)$ を示す．カオス同期が達成された後，復調信号 $t_2(k)$ が1ステップ前の情報信号 $s_1(k-1)$ に収束していることが分かる．情報信号 $s_1(k)$ がある場合とない場合の送信信号 $c_{12}(k)$ の振る舞いとそのパワースペクトルを**図2**と**図3**に示す．どちらの場合も送信信号はカオス的であり，そのパワースペクトルは全体的に少し異なるが，情報信号の周波数を推定することは全くできない．すなわち，情報信号がカオス的に変調されていることが分かる．

次に，システムパラメータのミスマッチについて考察する．サブシステム S_2 の同期化部は変更せずに，サブシステム S_1 の同期化部のみを以下のように変更する．

$$x_1(k+1)=1.4-1.01x_1^2(k)+y_1(k)+u_1(k)$$
$$y_1(k+1)=0.3x_1(k)$$

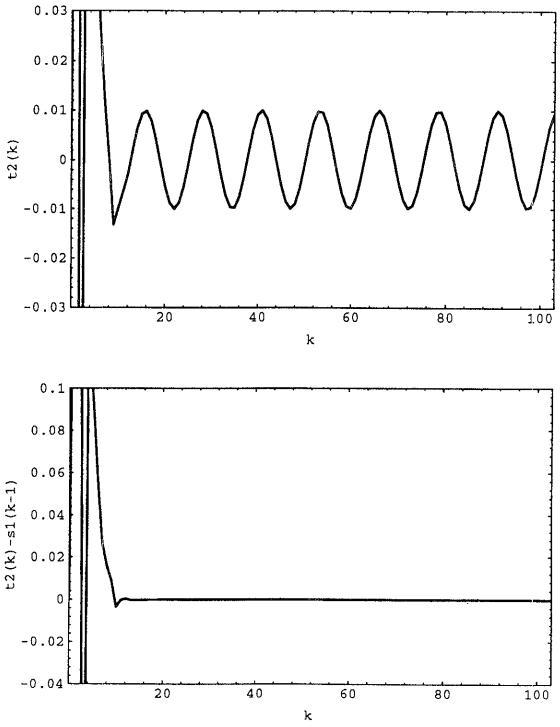


図1 復元信号 $t_2(k)$ とその情報信号との差 $t_2(k)-s_1(k-1)$ の振る舞い

Fig. 1 Behaviors of the demodulated signal $t_2(k)$ and the difference $t_2(k)-s_1(k-1)$ when the informational signal $s_1(k)=0.01sin0.5k$ is injected.

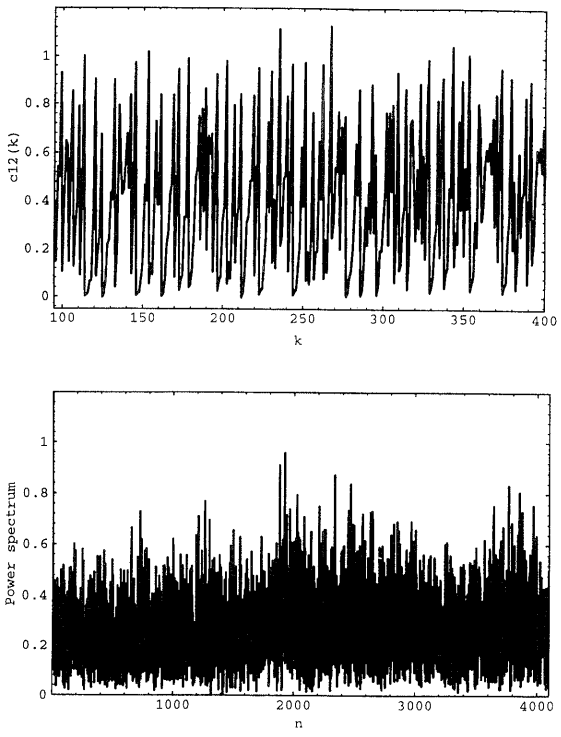


図2 送信信号 $c_{12}(k)$ の振る舞いとそのパワースペクトル

Fig. 2 Behavior and its power spectrum of the transmitted signal $c_{12}(k)$ with the informational signal $s_1(k)=0.01sin0.5k$.

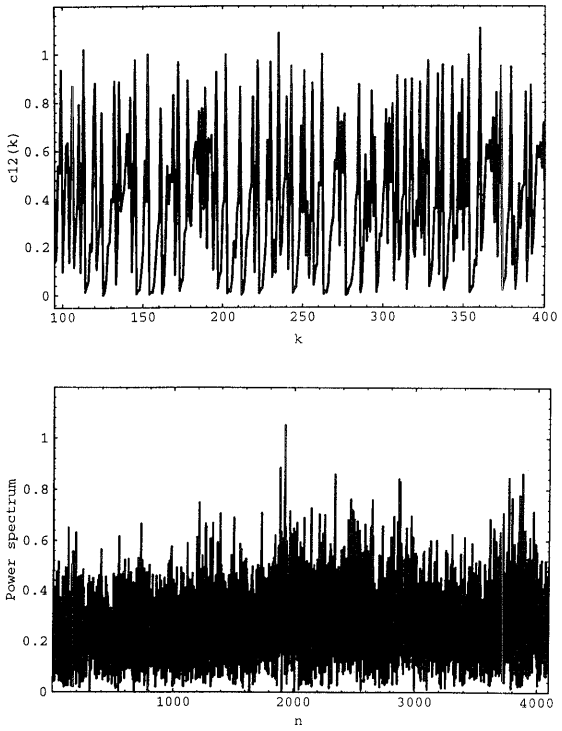


図3 情報信号がないときの送信信号 $c_{12}(k)$ の振る舞いとそのパワースペクトル

Fig. 3 Behavior and its power spectrum of the transmitted signal $c_{12}(k)$ without the informational signal.

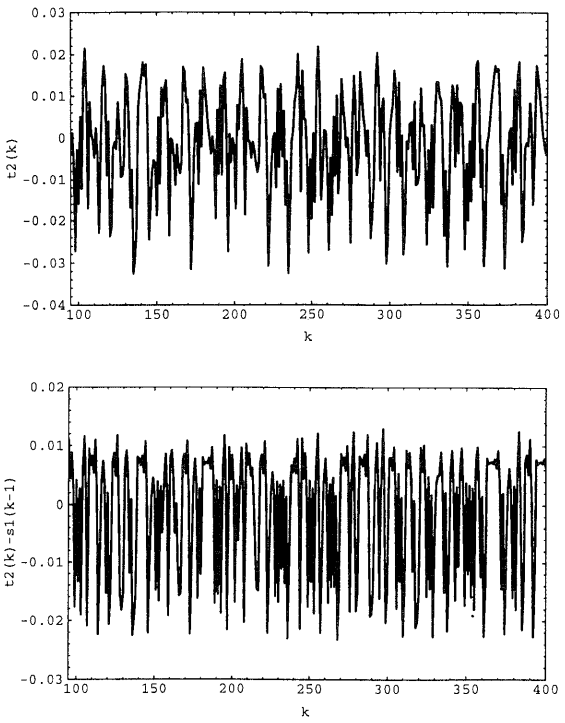


図4 同期部のパラメータにミスマッチがあるときの復元信号 $t_2(k)$ とその情報信号との差 $t_2(k)-s_1(k-1)$ の振る舞い

Fig. 4 Behaviors of the demodulated signal $t_2(k)$ and the difference $t_2(k)-s_1(k-1)$ in the case that the synchronization devices are mismatched.

すなわち，S_1 と S_2 の同期化部のシステムは第1式の $x_1^2(k)$ の係数が1%だけミスマッチしていることになる．情報信号として，式（9）を与えたときの復調信号 $t_2(k)$ およびその情報信号との差 $t_2(k)-s_1(k-1)$ の振る舞いを**図4**に示す．$x_1^2(k)$ の係数がわずか1%変動しただけで，図4に示すように，$t_2(k)-s_1(k-1)$ が0に収束しておらず，$t_2(k)$ の振る舞いも正弦波ではなく，カオス的になっていることが分かる．このように同期化部のパラメータがわずかにミスマッチしただけで，情報信号が受信側で復元されないことは，この通信システムの秘匿性が優れていることを表している．

5. おわりに

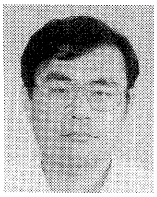
本論文では，カオス同期を達成するための制御則を提案し，その方法を秘匿通信に応用した．まず，サブシステムの状態の差に基づくフィードバック制御法を提案した．本手法が適用できるシステムのクラスには，LaiとGrebogiの方法で安定化できるシステムのクラスを含んでいる．さらに，彼らの方法ではヤコビ行列の計算が必要であるが，本手法では，このような計算を行うことなく制御系が構成できる．

次に，本手法を秘匿通信に応用した．カオスを利用した従来の秘匿通信法では，Pecoraらの方法をもとに，最初からカオス同期するようにサブシステムが構成されるために，駆動システムが固定されてしまい，1方向の通信しかできなかった．しかし，本手法では，通信方向に応じて，駆動システムを変更できるために，半2重通信が可能となる．また，同期化部として用いることのできるカオスシステムの次元に制限がないので，かなり多くのカオスシステムが同期化部に利用することができる．このことは，システムの秘匿性がかなり優れていることになる．ところで，通常，暗号解読の困難さは計算量と関連づけて論じられるが，カオスを用いた場合には，その解読困難性を表す指標がない．今後カオスを利用した秘匿通信が実用化するためには，この点が重要な検討課題である．さらに，実際に通信を行うときにはディジタル信号を符号化することになるが，このときの量子化誤差の影響についても今後の検討課題としたい．

参考文献

1) Pecora, L. M. and Carroll, T. L.: Synchronization in Chaotic Systems, *Physical Review Letters*, Vol. 64, No. 8, pp. 821-824 (1990).
2) Anishchenko, V. S., Safonova, M. A. and Sosnovtseva, O. V.: Synchronization and Stochastic Resonance in Chua's Circuit, *Proc. Workshop NOLTA '93*, pp. 81-86 (1993).
3) Carroll, T. L. and Pecora, L. M.: Cascading Synchronization of Chaotic Systems, *Physica*, Vol. D 67, pp. 126-140 (1993).
4) Ott, E., Grebogi, C. and Yorke, J. A.: Controlling Chaos, *Physical Review Letters*, Vol. 64, No. 11, pp. 1196-1199 (1990).
5) Mehta, N. J. and Henderson, R. M.: Controlling chaos to Generate Aperiodic Orbits, *Physical Review A*, Vol. 44, No. 8, pp. 4861-4865 (1991).
6) Lai, Y.-C. and Grebogi, C.: Synchronization of Chaotic Trajectories Using Control, *Physical Review E*, Vol. 47, No. 4, pp. 2357-2360 (1993).
7) 潮 俊光：一様な結合をもつ大規模システムにおけるカオスの安定化フィードバック，信学技報，NLP 91-41 (1991).
8) Ushio, T.: Control for Chaotic Synchronization in Uniformly Connected Systems, *Proc. NOLTA '93*, Vol. 1, pp. 63-66 (1993).
9) 潮 俊光：複合システムにおけるカオス同期化制御，信学技報，NLP 93-90 (1994).
10) 潮 俊光：1次元1方向結合のカオスニューラルネットワークにおけるカオスの同期化，信学技報，NLP 93-50 (1993).
11) 潮 俊光：1次元双方向結合カオスニューラルネットワークのカオス同期化と制御，信学技報，NLP 93-76 (1994).
12) 伊藤，村上，Halle, K. S., Chua, L. O.：カオスの同期を用いた信号の伝送，信学技報，CAS 93-39/NLP 93-27 (1993).
13) Cuomo, K., Oppenheim, A. V. and Strogatz, S. H.: Synchronization of Lorenz-Based Chaotic Circuits with Application to Communications, *IEEE Trans. Circuits and Systems-II*, Vol. 40, No. 10, pp. 626-633 (1993).
14) Dedieu, H., Kennedy, M. P. and Hasler, M.: Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-synchronizing Chua's Circuits, *IEEE Trans. Circuits and Systems-II*, Vol. 40, No. 10, pp. 634-642 (1993).
15) Hasler, M., Dedieu, H., Kennedy, M. P. and Schweizer, J.: Secure Communication via Chua's Circuit, *Proc. Workshop NOLTA '93*, pp. 81-86 (1993).
16) 伊藤，村上：離散力学系の同期現象とセキュリティ通信，信学技報，NLP 92-50 (1992).
17) Kasai, H., Senmoto, S. and Matsushita, M.: PCM Jitter Suppression by Scrambling, *IEEE Trans. Comm.*, Vol. COM-22, No. 8, pp. 1114-1122 (1974).
18) Lee, B. G. and Kim, S. C.: *Scrambling Techniques for Digital Transmission*, Springer (1994).

(平成6年7月17日受付)
(平成7年1月12日採録)



潮 俊光（正会員）

1958年2月28日生．1980年神戸大学工学部システム工学科卒業，1985年同大学博士課程修了．同年よりカリフォルニア大学バークレイ校研究員．1986年より神戸大学工学部システム工学科助手，1990年神戸女学院大学家政学部講師，助教授を経て，1994年より大阪大学工学部電子工学科助教授となり現在に至る．非線形振動の解析，離散事象システムの制御に関する研究に従事．学術博士．電子情報通信学会，計測自動制御学会，システム制御情報学会，人工知能学会，IEEE, ACM などの会員．