L-036

カオス発生回路を用いた秘匿通信システム
The Secrecy Communication System Using Chaos Generating Circuit

清水 能理
Yoshimasa Shimizu

1．はじめに

カオスは,決定論的法則に従う非線形の効果により複雑な振る舞いをする。特徴として,振る舞いが複雑でありながら,法則によってその複雑さが生み出されるということがあげられる[1,5]。
人工的にカオスを発振させる場合を考えると,ローレンツ・モデルやエノン写像といった解析的な式で定義された力学系を用いるのが一般的である。現在カオスを発振させるために利用されるカオスモデルは種々あるが,自然界における多様なカオスに対し,カオスモデルを用いて人工的に作り出されるカオスは限定的なものである[1,4]。工学において,多様なカオス応用を実現するには,人工的にカオスを発振させる電子回路の実装が不可欠である。カオスの生じる電気回路として,既にダフィング方程やファン・デル・ポールの発振回路,ダイオード回路を用いたものなどが知られている[1]。本研究では,カオス発生回路として,負性抵抗を有する Chua 回路に注目する。

また,カオス力学系を記述する微分・差分方程式において,パラメータがある一定の値を超えると解の数が変わり,解が定性的に変化する現象を分岐と呼ぶ[5]。カオスモデルでは,分岐が起こる分岐パラメータの値により軌道の位相的性質を変える現象が起こる。カオス挙動を示しているときは多くの不安定周期点を持っているが,パラメータのとる値によっては系がカオスとなる値の範囲で周期性を示す窓を生じる場合がある[4,5]。そのためカオスを利用したシステムにおけるパラメータの設定には十分注意しなければならない。

一方,統計的解析におけるブートストラップ法に類似の概念を持つ,サロゲートデータ法(the method of surrogate data)と呼ばれるカオス性の検定手法が提案されている[3]。そこで,数値実験を行い,分岐図を用いてカオスを発振するパラメータを推定し,サロゲートデータ法を応用して決定する。また,数値実験により,カオス分岐におけるカオス性の考察を行う。

2．問題提起

分岐パラメータに関して,分岐図を用いて系がカオスとなるパラメータ値を探索する方法を考える。

はじめに,簡単な法則に従っていながら複雑なカオス挙動を示す端的な例である,ロジスティック写像を例に用いて分岐図について考える。分岐図とは,分岐パラメータを変化させた場合に起こる分岐を図に表わしたものである[1,4]。ロジスティック写像の分岐図は横軸に分岐パラメータ r,縦軸に周期点をとる。このときのロジスティック写像の方程式は次式となる。

$$\left.\begin{aligned} X_{n+1} &= aX_n(1-X_n) \\ 0 \le a \le 4, &0 \le X_0 \le 1 \end{aligned}\right\} \qquad (1)$$

ここで,X(n)はこの式の変数であり０から１の間で定義されている。a は０から４までの値をとる任意の定数である。

八戸工業大学, Hachinohe Institute of Technology

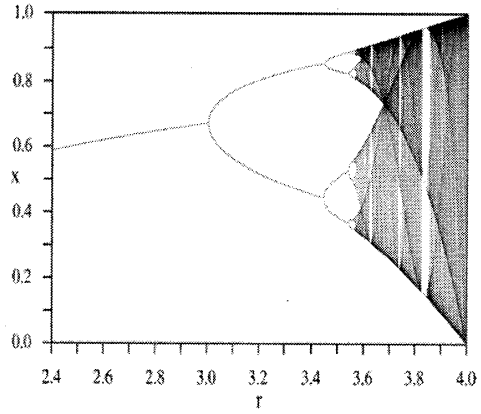

図 1　ロジスティック写像の分岐図

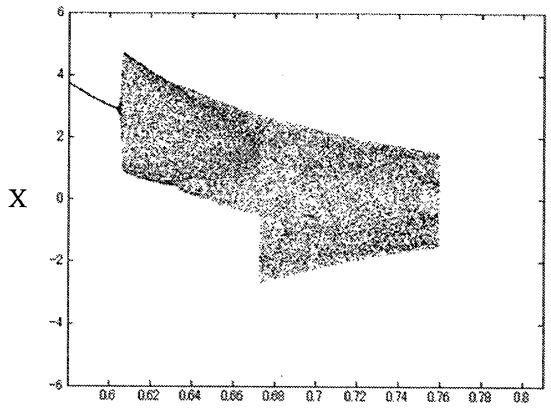

図 2　Chua 回路の分岐図

図 1 のロジスティック写像の分岐図では,カオス的振る舞いをする値の領域において,周期性を示す窓の存在を確認することができる。

次に,Chua 回路の分岐図について考える。このとき,回路の方程式は次式で与えられる。

$$\left.\begin{aligned} c_1\frac{dV_1}{dt} &= G(V_2 - V_1) - g(V_2) \\ c_2\frac{dV_2}{dt} &= G(V_1 - V_2) + I \\ L\frac{dI}{dt} &= -V_2 \end{aligned}\right\} \quad (2)$$

$$g(V_1) = m_0V_1 + \frac{1}{2}(m_1 - m_0)|V_1 + B| + \frac{1}{2}(m_0 - m_1)|V_1 - B| \quad (3)$$

ここでは, 常微分方程式の近似解を求める方法の 1 つである, 4 次の Runge-Kutta 法を用いてシミュレーションを行った。扱う Chua 回路の分岐図は,横軸に分岐パラメータ値 G,そして縦軸に状態 x の値をとる。

Chua 回路の分岐図について見ると,系がカオス的振る舞いをする領域は推定できるが,窓の存在を確認し難いという問題が生じることがわかる。パラメータの設定によっては,系がカオスと思われる値を設定しても,実は窓である可能性がある[4,5]。したがって,Chua 回路を用いたシステムを考える場合,パラメータ値を設定する際にカオス性の検定を行う必要性がある。

3．サロゲートデータ法[3]

カオス応答を示すための重要な要因は非線形性にある。サロゲートデータ法では,観測された時系列信号に対する線形確率過程の存在を帰無仮説として提示し,ある非線形統計量の推定を通じて検定する。そして,帰無仮説を棄却することで時系列信号における非線形の存在を示す。

非線形性を示すと考えられる時系列信号に対しては,種々の帰無仮説を考えることができるが, 線形確率過程の存在を基盤とした帰無仮説を用いるのが自然である。実際に掲示される典型的な仮設は,

(1) 時間的に全く無相関な(白色な)データであった。

(2) 時間的には線形相関を持つような(有色された)データであった。
(3) 時間的には線形相関があるようなデータ,ある種のスタティックで単調な非線形変換により観測することで得られたデータであった。

である。サロゲートデータ法では,上述の帰無仮説に従うようなサロゲートデータを多数作りだし,これらの統計的性質がオリジナルデータのそれと異なることを検定する。

これらの帰無仮説に基づいた時系列信号をサロゲートデータ(surrogate data)と呼ぶ。また,これらのサロゲートデータを作り出す基本アルゴリズムは,各々,

(1) ランダム・シャッフル(random shuffle,以下 RS),
(2) フーリエ・トランスフォーム(Fourier transform,以下 FT),
(3) アンプチュード・アジャステッド・フーリエ・トランスフォーム(amplitude adjusted Fourier transform,以下 AAFT),あるいは,ガウシアン・スケーリング(Gaussian scaling)

アルゴリズムと呼ばれている。

4．提案手法

提案する Chua 回路の分岐パラメータ値設定手法を以下にまとめる。

(1) Chua 回路における分岐パラメータ G の値を変化させて行き,各値のときの Chua 回路から出力される時系列信号を計算する。
(2) 横軸に G の値,縦軸に出力信号の状態を取る。各 G の値において,(1)で得られた信号の値を重ねてプロットし,カオス分岐図を作成する。
(3) 手法(2)で作成した分岐図の形態をもとに,時系列がカオス的振舞いをする領域の分岐パラメータ値の範囲を推定する。
(4) 推定した領域において特定した分岐パラメータ値を用いたときの時系列データに対して,サロゲート法を適用し,そのシミュレート結果からカオスか否かの検定を行う。

5．秘匿通信システムへの応用

高度情報化社会へと移行し、安全なネットワーク通信、電子情報の保護は重要な課題である。現在ネットワーク上の電子情報を保護する暗号化プロトコルとして SSL、TLS、S/MIME などが用いられている。これらで用いられている公開鍵暗号方式は、素因数分解や離散対数問題などを応用したものが主に用いられているが、昨今のコンピュータの処理速度の上昇により、今後さらに暗号鍵長の増加が必要とされており、コンピュータへの負担がより一層増加すると予想される。よって、単純規則に従うシンプル性を有しながらも複雑不規則な現象を生じるカオス現象を応用する。暗号化関数の利便性、暗号鍵の秘匿性、秘匿通信システムのモデルの秘匿性を解決するため、カオス同期およびカオス分岐に基づいた搬送波の生成および暗号方式を用いた秘匿通信システムを構築できる。

カオス分岐を行った変調部の状態は、カオス性を保持していなければならないので、分岐パラメータの範囲を検証する必要がある。よって、サロゲート法によるカオス性の検定と分岐図を用いたカオス分岐パラメータの範囲設定を行えばよい。カオス同期化部の状態を暗号鍵として用いてカオス分岐を発生させたカオス波形に基づいた暗号化関数を設計し、暗号化・復号を行うようにする。従来の手法のように、暗号化関数を複雑に

する必要がなく、その逆関数を求める困難さが小さい。

6．シミュレーション

ここでは,図 2 の Chua 回路の分岐図を用いてカオス発振回路のパラメータ値を推定する。分岐図を見ると,分岐パラメータが 0.60 の値を過ぎた辺りから,軌道の位相的性質が変化していることが伺える。位相的性質の変化が見られる分岐パラメータの値について,位相関係を示したものが図 3~7 である。分岐図から考えると,分岐パラメータが 0.70 付近の値がパラメータの設定値として妥当であると推定でき,図 6 から実際に分岐パラメータ値が 0.70 のときに,ダブルスクロールアトラクタを形成していることがわかる。

次に,推定したパラメータ値における時系列データに対して FT サロゲートデータ法を適用した数値実験を行い,カオス性の検定をした。

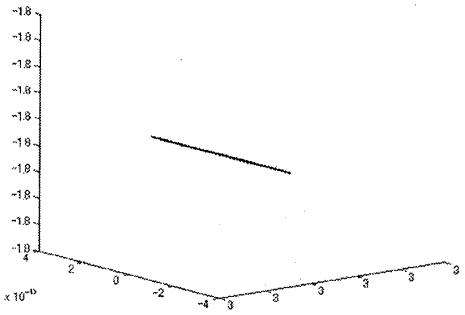

図 3　分岐パラメータ 0.6 における位相図

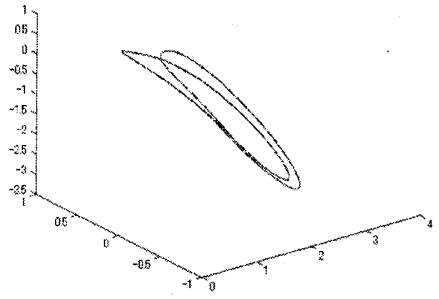

図 4　分岐パラメータ 0.64 における位相図

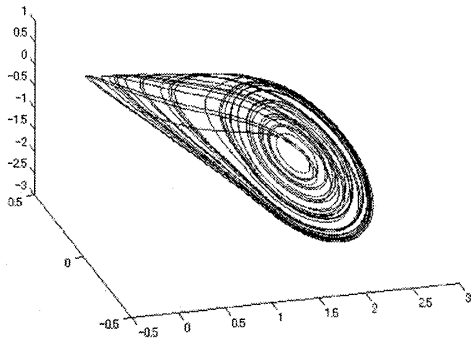

図 5　分岐パラメータ 0.67 における位相図

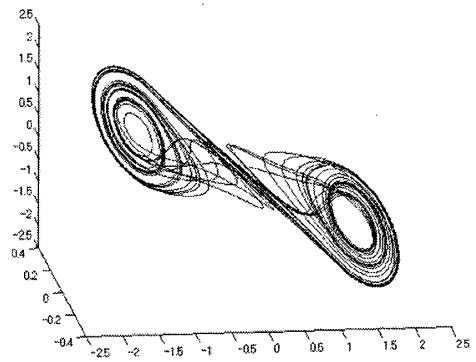

図 6　分岐パラメータ 0.70 における位相図

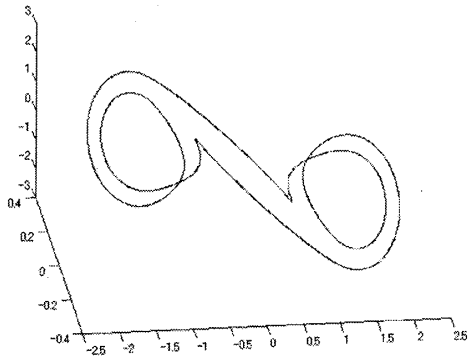

図 7　分岐パラメータ 0.6981 における位相図

カオスを発振する分岐パラメータ値を推定したのち,設定したパラメータ値の Chua 回路から出力として得られる時系列信号に対して時系列解析を行い,カオス性を有することを示す[3]。前述のとおり,カオスを発振する領域のパラメータ値を設定したつもりが,窓である場合も考えられる[4,5](図 7)。 以下に数値実験で用いたパラメータ G=0.70 と G=0.6981 における Chua 回の x 値の時系列信号,パワースペクトル,頻度分布を示す。

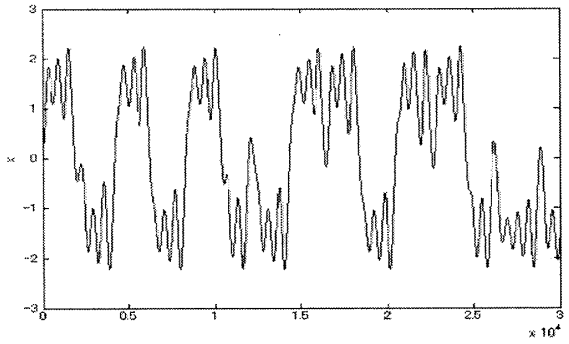

図 8 Chua 回路における時系列信号(G=0.70)

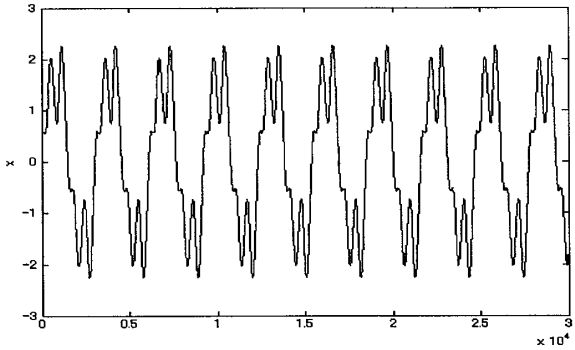

図 11 Chua 回路における時系列信号(G=0.6981)

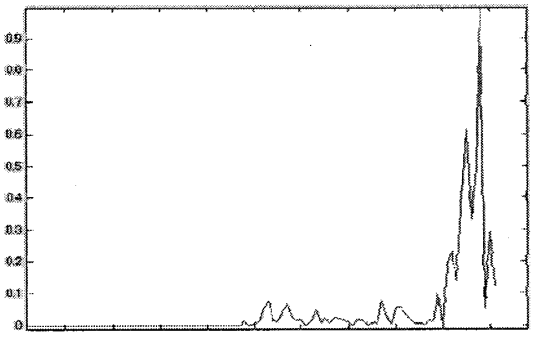

図 9 時系列信号のパワースペクトル(G=0.70)

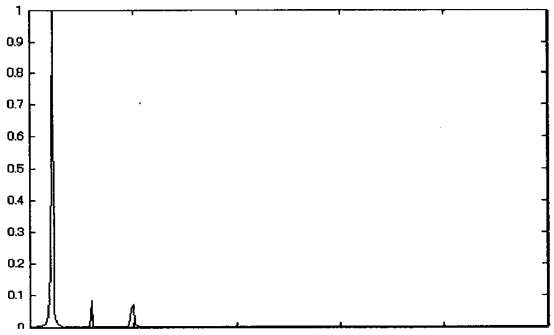

図 12 時系列信号のパワースペクトル (G=0.6981)

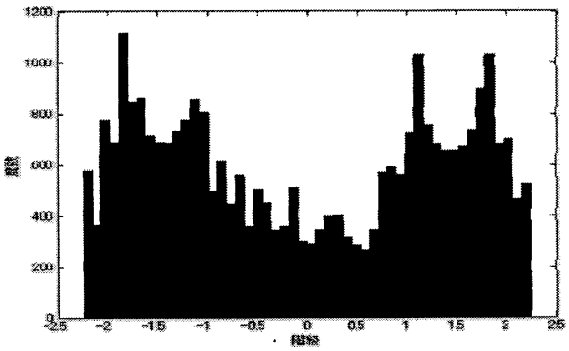

図 10 時系列信号の度数分布(G=0.70)

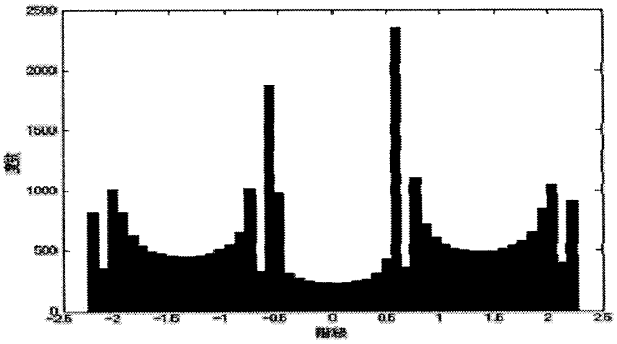

図 13 時系列信号の度数分布(G=0.6981)

6.1 FT サロゲート法を用いた数値実験果

Chua 回路の時系列信号に対し、FT サロゲート法を適用した数値実験例の結果を示す。

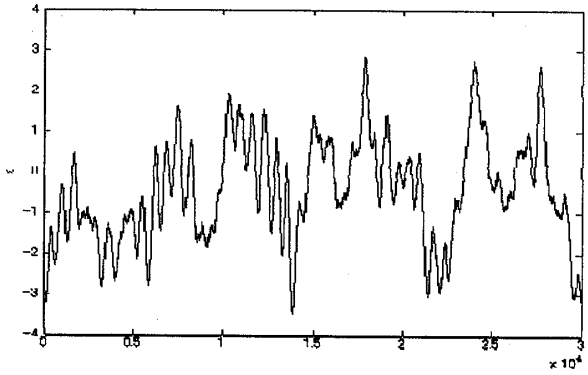

図 14 FT サロゲート変換信号(G=0.7)

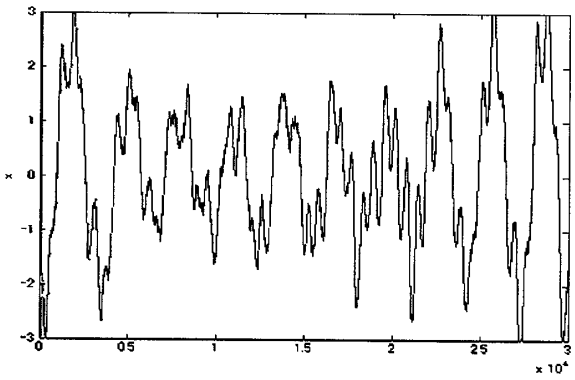

図 17 FT サロゲート変換信号(G=0.6981)

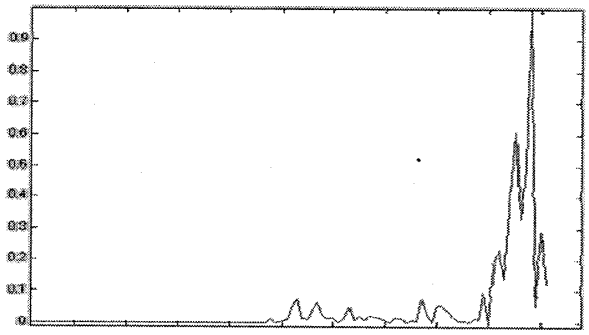

図 15 変換信号のパワースペクトル(G=0.70)

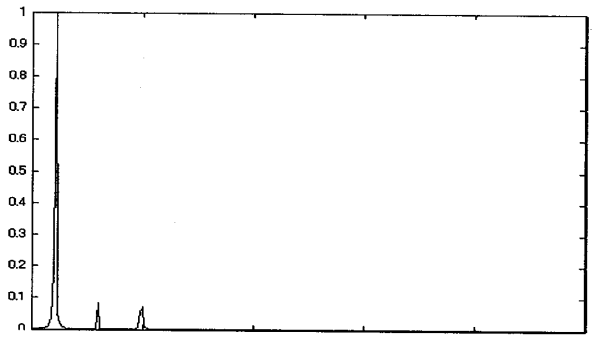

図 18 変換信号のパワースペクトル(G=0.6981)

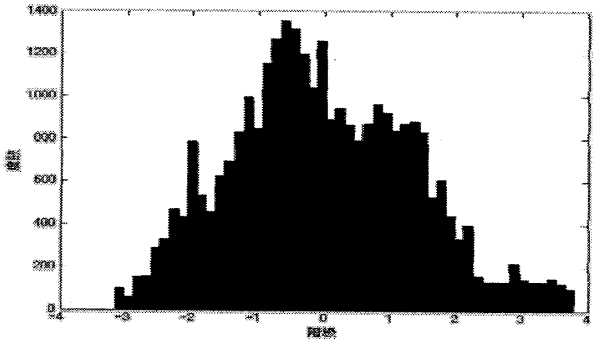

図 16 変換信号の度数分布(G=0.70)

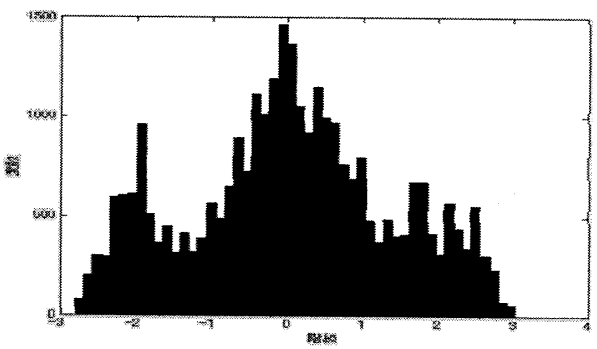

図 19 変換信号の度数分布(G=0.6981)

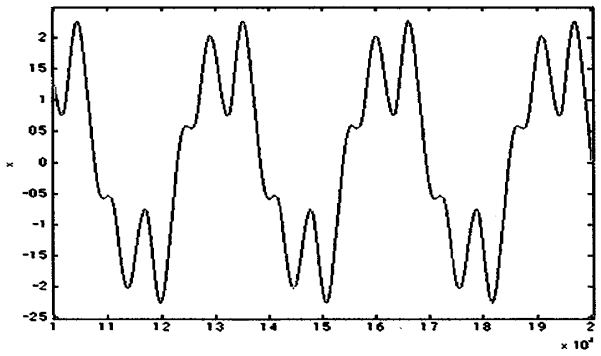

図 20　Chua 回路における時系列信号の拡大
(G=0. 6981)

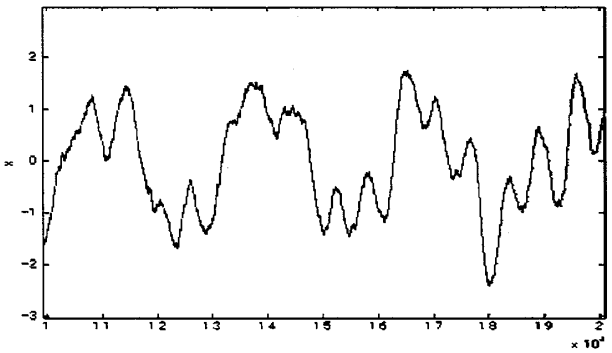

図 21　FT サロゲート変換信号の拡大
(G=0. 6981)

表 1　FT サロゲートデータ作成過程において保存される統計量

平均	分散	頻度分布	自己相関
○	○	×	○

※保存される○　保存されない×

オリジナルデータとサロゲートデータの統計量を比較すると,表 1 にまとめたとおり平均,分散ともにサロゲートデータ作成過程において統計量が保存されていた。一方,FT アルゴリズムの性質上,頻度分布は保存されない[3](図 16)。図 8 と図 14 の信号を比べると,オリジナルデータ時系列信号の構造は全く壊されている。これにより,分岐パラメータが 0.70 値をとる場合,時系列信号は線形なダイナミクスで表現することが難しいことがわかる。

分岐パラメータ 0.6981 をとる場合のオリジナルデータとサロゲートデータの統計量を比較すると,平均,分散ともにサロゲートデータ作成過程において統計量が保存されていた。同様に,FT アルゴリズムの性質上,頻度分布は保存されない[3](図 19)。図 11 と図 17 の信号を比べると,オリジナルデータ時系列信号と FT サロゲートデータ変換信号の構造は破壊されていない。これにより,分岐パラメータが 0.6981 値をとる場合,線形なダイナミクスで表現できる可能性が高いことが推察できる。

7．考　察

数値実験では,Chua 回路において分岐図を参考にし,カオスを発振する領域から分岐パラメータ 0. 70 値と 0. 6981 値 2 つのパラメータを推定した。そして,推定した分岐パラメータ値の Chua 回路から出力として得られる時系列信号に対し時系列解析を行った。

FT サロゲートデータ法の実験結果から,分岐パラメータ 0. 70 値のときにカオス性を有する可能性があり,0. 6981 値のときカオスの窓であることが確認できた。よって, 0. 70 値のときはカオスで,0. 6981 値のときは窓である。

このことから,Chua 回路のカオスを発振する領域のパラメータ値を設定した場合,窓であるかを確認するには,サロゲート法を用いることが有効である。

8．まとめ

カオス分岐図を用いて設定した分岐パラメータ値における Chua 回路からの出力としての時系列信号に対して,サロゲートデータ法を適用し,カオス性の検定を行った。特定パラメータ値における Chua 回路からの出力がカオス的であることを示すと同時に,カオスの窓の存在を確認することができた。

よって,Chua 回路のカオス分岐パラメータの探索には,分岐図からのカオス領域の推定とサロゲートデータ法を応用したカオス検定が有効であることがわかった。

カオス通信は、システムのカオス性が保証されなければならない。よって、カオス同期化部の状態を暗号鍵として用い、変調部、復調部にカオス分岐を発生させる Chua 回路を用いた秘匿通信システムにおける分岐パラメータの探索は、サロゲートデータ法を用いることが有効である。

参考文献

[1] 鈴木 昱雄：カオス入門, コロナ社, 2000

[2] 鈴木 昱雄：Mathematica3.0 によるカオス工学への応用, コロナ社, 2000

[3] 合原 一幸, 池口 徹, 山田 泰司, 小室 元政：カオス時系列解析の基礎と応用, 産業図書, 2000

[4] 合原 一幸：カオスセミナー, 海文堂出版, 1994

[5] 下條 隆嗣:Mathematica シミュレーション物理学 6・カオス力学入門, 近代科学社, 1992

[6] 潮 俊光：カオス通信への応用, 電子情報通信学会論文誌 A, VolJ82-A, pp.1801-1807, 1999

[7] 徳田 功, 宮野 尚哉, 合原 一幸:サロゲートデータ法に基づく持続発生母音の基本周期揺らぎの高次相関解析, 電子情報通信学会論文誌 A, VolJ87-A, pp.335-363, 2004

[8] M.Kuramatu, K.mori: “A Simple Electric Circuit Generating Chaos,” The institute of electronics, information and communication engineers, Vol.93, No.452, pp.31-38, 1994

[9] Y.Shimizu: “Application of the Variable Structure Servo Control to Chaotic Dynamics Systems,” The Bulletin Of Hachinohe Institute of Technology, No.27, pp.97-112, 2008