計測自動制御学会東北支部 第258回研究集会(2010.6.24)
資料番号 258-11

時系列の定量分析を用いたカオス通信系構築

Building Chaotic Communication system Using Quantitative Analysis of Time Series

○佐々木　章寛、 清水　能理
Akihiro Sasaki、Shimizu Yoshimasa
八戸工業大学
Hachinohe Institute of Technology

キーワード: カオス(Chaos)、サロゲート(Surrogate)、統計量(Statistics)

連絡先: 〒031-8501　青森県八戸市妙字大開88-1 八戸工業大学工学部システム情報工学科清水研究室
清水能理　Tel: 0178-25-8135　Fax: 0178-25-1691　E-mail: shimizu@hi-tech.ac.jp

１．まえがき

ネットワーク上の電子情報を保護する公開鍵暗号方式は、素因数分解や離散対数問題などが用いられているが、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、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。暗号化関数の利便性、暗号鍵の秘匿性、通信系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く搬送波生成および暗号方式を用いた秘匿通信系が提案されている。カオスモデルは種々あるが、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。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考案されている。そこで、カオス発信回路における有効なパラメータ値を、カオス分岐図を用いて設定し、得られた時系列信号に対してサロゲートデータ法に基づいたカオス性の判定を行う。

２．カオス同期秘匿通信システム

対象とする秘匿通信系は、カオス発生回路の Chua 回路を用いたカオス変調通信系である。サブシステム S1、S2 には、同期部、変調部、復調部を設計する。同期部はカオス同期化制御を行い、S1、S2 の状態を等しくする。通信時の秘匿性を高めるため、変調部、復調部のカオス状態に対し、同期部の状態を暗号鍵として用いてカオス分岐を行う。カオス分岐を行うために用いるカオス同期部の状態、およびカオス分岐を行った変調部の状態は、カオス秘匿通信の特性上カオス性を保持していなければならない。変調部では、カオス分岐を発生させた変調部の状態を用いて、情報信号を暗号化関数により搬送波に変換し、送信する。図１の Chua 回路を用いて、図２の秘匿通信システムを構成する。送受信の各サブシステムに同期化部、変調部、復調部を設計する。

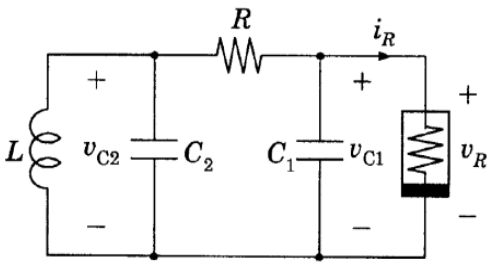

図１　Chua 回路構成図

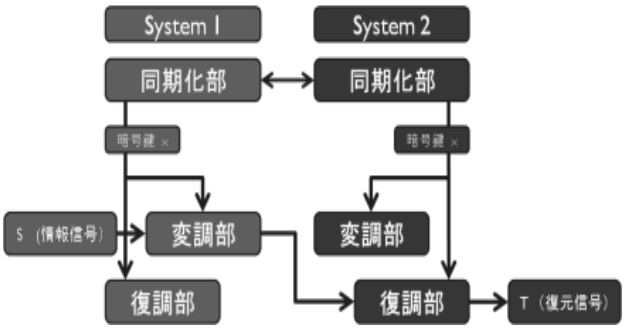

図 2　秘匿通信システム

3．問題の記述

秘匿通信系のカオス時系列は、変調部と復調部ともに同様のカオス性が必要となる。カオスモデルは、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（カオス分岐)。カオス挙動を示すとき、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周期性を生じる（カオス窓)。カオス状態はその複雑さゆえ高い秘匿性をもち、秘匿通信システムに応用される。しかし、人工的にカオスを発振させる電子回路の実装において、分岐に基づきパラメータ値の設定するとき、カオス窓の問題に注意を払わなければならない。

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。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。

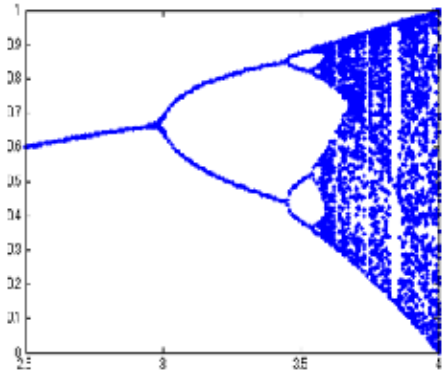

図 3　ロジスティック写像の分岐図

図 3 のロジスティック写像の分岐図は横軸に分岐パラメータ、縦軸に周期点をとったものである。このときのロジスティック写像の方程式は（1）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。

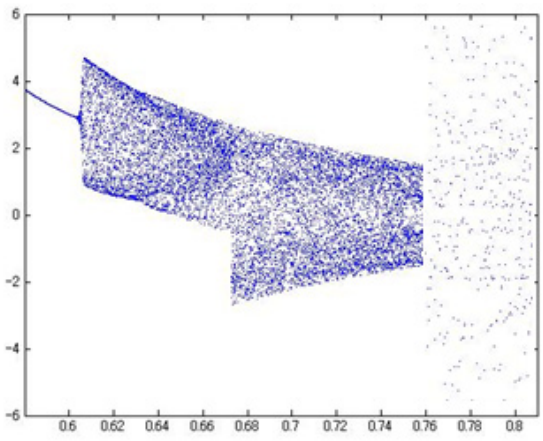

図 4　Chua 回路の分岐図

図 4 の Chua 回路の分岐図は、横軸に分岐パラメータ、縦軸に状態 x 値をとったものである。図 3 のロジスティック写像の分岐図は離散時間で窓が確認できるが、図 4 の Chua 回路の分岐図では連続時間で窓が確認し難い。このように、分岐図を用いた視覚的探索によるパラメータ値の設定をする際に、窓の予測困難性があげられる。したがって、Chua 回路を用いたシステムのパラメータ値を設定する場合、カオス性の検定を行う必要性がある。

4．サロゲート法

カオスかランダムノイズかの判断の重要な要因の一つに非線形性がある。時系列信

号が非線形を有することを示すのは、時系列信号がカオスであることを示すよりも容易である。そこで、時系列信号に対する線形性を主体とした帰無仮説を採用し、これを棄却できれば、カオス時系列解析を用いて推定された特徴量の信頼性を向上できると考えられる。サロゲートデータ(surrogate data)法は、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帰無仮説を検定し棄却することで、時系列信号を生み出したダイナミクスにおける非線形の存在を示すのである。具体的に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で或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出し、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サロゲートデータを作り出す基本アルゴリズムは、

(1)RS(Random Shuffle)サロゲートデータ:「観測された時系列信号は、時間的に全く無相関である」という帰無仮説に従う

(2)FT(Fourier Transform)サロゲートデータ:「観測された時系列信号は、時間的に線形相関を持つ確率的データである」(頻度分布が保存されない) という帰無仮説に従う

(3)AAFT(Amplitude Adjusted Fourier Transform) サロゲートデータ (ガウシアン・スケーリング(Gaussian Scaling)アルゴリズムとも呼ばれている):「観測された時系列信号は、非線形確率過程から作り出されたが、観測する際に性的な単調非線形変換を施されたことにより得られたデータである」という帰無仮説に従う、である。

さらに、改良型のアルゴリズムがある。

(4)FS(Fourier Shuffle)サロゲートデータ:前述の FT アルゴリズムは、その作成手順からパワースペクトルは完全に保存するものの、頻度分布を全く保存しないという特徴を有する。このことは、FT サロゲートでは、オリジナルの時系列信号には存在し得ない頻度分布を実現してしまうということを意味し、FT サロゲートのアルゴリズムを用いれば負の値も出現する。そこで、サロゲートデータ作成のアルゴリズムとして、フーリエ・シャッフル(Fourier shuffle、以下 FS)アルゴリズムと呼ばれるサロゲートデータ作成のアルゴリズムが提案されている。FS サロゲートは、サロゲートデータをオリジナルデータに従うように並べ換える。その結果、FS サロゲートは、オリジナルデータと同じ頻度分布を、つまり 1 次統計量及び 2 次統計量のうち分散を完全に保存する。また、2 次統計量としての相関関数もほぼ保存される。

(5)IAAFT (Iterative Amplitude Adjusted Fourier Transform)サロゲートデータ:前述の AAFT サロゲートアルゴリズムでは、時系列データが有限である場合、相関関数などの 2 次統計量は完全に保存されない。サロゲートデータ法を導入する目的は、従来の時系列解析で用いられてきた自己相関関数を主体とする手法では非線形性を扱えないということを統計的に定量化することである。この観点からすると、1 次統計量を完全に保持することだけでなく、2 次統計量もオリジナルデータのそれに近いこと、もしくは同じことが望ましい。このような考え方に基づいて、自己相関関数の差がより小さいサロゲートデータを作成するために、イタレイティブ・AAFT サロゲートデータ(Iterative AAFT、以下 AAFT)アルゴ

リズムが提案されている。

５．提案手法

カオス発振回路のパラメータ値の推定にはカオス分岐図を用いることが考えられるが、周期軌道（窓）が発生していないかのカオス性評価が必然となる。よって、確率・統計論に基づいた時系列解析手法のサロゲートアルゴリズムに基づくカオス性検定と分岐図を応用したカオス分岐パラメータ値の範囲設定を行う。分岐パラメータ設定手法について、以下にまとめる。

(1) Chua 回路における分岐パラメータの値を変化させていき、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) 横軸に分岐パラメータの値、縦軸に出力信号の状態を取る。各パラメータ値において、(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) (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、カオス窓か否かの検定を行う。

秘匿通信システムでは、変調部でカオス分岐を行った状態はカオス性を保持していなければならない。よって、分岐図を用いたカオス分岐パラメータ値の範囲で、サロゲート法によるカオス性の検定を行う。カオス同期化部のカオス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。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

カオス時系列解析システムであるソフト ChaosTimes を利用して求めた Chua 回路分岐パラメータ値 0.70 と 0.6981 をとる場合の状態 x の時系列信号と、各サロゲートデータ変換信号を計算した。図 5 は PC 用の Sunday ChaosTimes である。

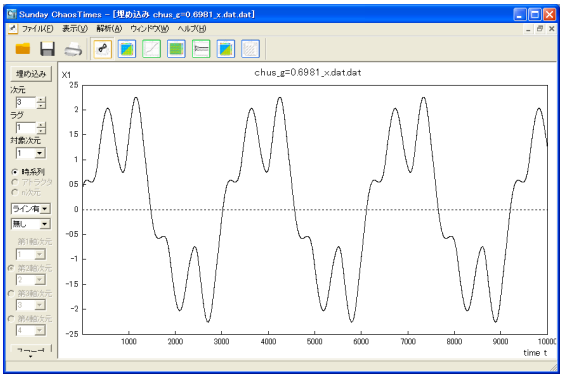

図 5　Sunday ChaosTimes の実行画面

FT サロゲート法を用いた数値実験結果の例を以下に示す。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 のように平均、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。図 6 と図 7 の信号を比較すると、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。このことから、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。

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×

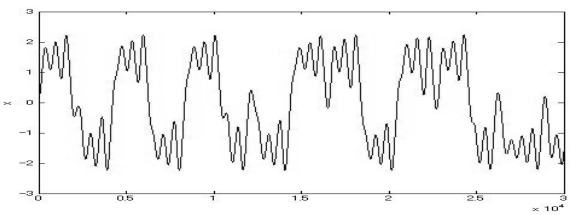

図 6　Chua 回路における時系列信号

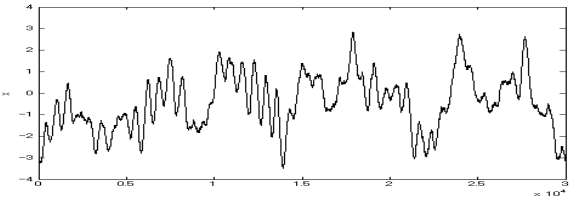

図 7　FT サロゲート変換信号

表 2　周期性とフラクタル性

分岐パラメータ	周期性	フラクタル	カオス性
G=0.70	○	○	○
G=0.6981	○	○	×

表 3　カオス性の有無

アルゴリズム	G=0.70	G=0.6981
RS サロゲート	○	×
FT サロゲート	○	×
AAFT サロゲート	○	×
FS サロゲート	○	×
IAAFT サロゲート	○	×

○：カオス性の示唆　×：カオス性の否定

7．まとめ

カオス発生回路として、負性抵抗を有する Chua 回路に注目した。周期性、フラクタル性を実験から確認できた。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 回路からの時系列信号に対し、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ことができ、サロゲートデータ法を用いたカオス検定は有効であった。

参考文献

[1] 合原一幸:カオスセミナー,海文堂出版,1994

[2] 潮 俊光:カオス制御,カオス全書 4,朝倉書店,1996

[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

[3] 鈴木 昱雄:カオス入門,コロナ社,2000

[4] 合原一幸:カオスセミナー,海文堂出版,1994

[5] 藤井恭平,清水能理:カオス発生回路を用いた秘匿通信システムの製作,平成 20 年度第 1 回情報処理学会東北支部研究会,講演資料,セッション 1,講演番号 4, 2008.12

[6] 目黒友紀,清水能理:カオス制御を応用したカオス同期化システム,平成 20 年度第 2 回情報処理学会東北支部研究会,講演資料,セッション 2,講演番号 9,2008.12

[7] 元井和征,清水能理:カオス分岐と窓に関する考察,平成 20 年度第 4 回情報処理学会東北支部研究会,講演資料,2009.2

[8] カオス時系列解析システム ChaosTimes http://www.aihara.co.jp/rdteam/chaostimes/index-j.html

[9] Sunday ChaosTimes による解析の実例 http://www.aihara.co.jp/rdteam/sunday-chaostimes/sundayct-examples.pdf#search='sunday chaos times'