

カオスダイナミクスの分離を利用した誤り訂正手法の 送信信号数に対する性能評価

荒井伸太郎[†] 西尾 芳文^{††} 山里 敬也^{†††}

[†] 香川高等専門学校 〒 769-1192 香川県三豊市詫間町香田 551

^{††} 徳島大学 〒 770-8506 徳島市南常三島 2-1

^{†††} 名古屋大学 〒 464-8603 名古屋市千種区不老町 C3-1(631)

E-mail: [†]arai@cn.kagawa-nct.ac.jp, ^{††}nishio@ee.tokushima-u.ac.jp, ^{†††}yamazato@nagoya-u.jp

あらまし カオス系列によって変調された信号のみを用いて復調を行うノンコヒーレントカオス通信システムは、カオスの特徴を活かした独特の通信システムとして知られている。しかしながら、一般的な通信システムと比較すると、通信特性は劣るため、ノンコヒーレント通信の特性向上のためには、カオスの特徴を利用したさらなる工夫が必要である。私達はこれまでの研究で、カオスダイナミクスの分離・再構成を利用した誤り訂正手法を提案した。シミュレーションを行った結果、従来手法(誤り訂正無し)と比較して、BER 特性において2~2.5 dBの利得が得られた事を確認した。本稿では、カオスダイナミクスの分離・再構成による効果をより詳細に解析するために、本誤り訂正手法の性能評価を行う。具体的には、一度に送信される信号ブロック数とその信号の組み合わせに注目し、誤り訂正能力の解析を行う。

キーワード カオス, ノンコヒーレントカオス通信システム, 誤り訂正, カオスダイナミクス

Performance Evaluation of Error-Correcting Scheme Using Separation of Chaotic Dynamics for Number of Transmitting Data

Shintaro ARAI[†], Yoshifumi NISHIO^{††}, and Takaya YAMAZATO^{†††}

[†] Kagawa National College of Technology, 551 Kohda, Takuma-cho, Mitoyo, Kagawa, JAPAN

^{††} Tokushima University, 2-1 Minami-Josanjima, Tokushima, JAPAN

^{†††} Nagoya University, Furo-cho, Chikusa-ku, Nagoya, JAPAN

E-mail: [†]arai@cn.kagawa-nct.ac.jp, ^{††}nishio@ee.tokushima-u.ac.jp, ^{†††}yamazato@nagoya-u.jp

Abstract Noncoherent chaos communications, which do not need to use basis signals (unmodulated carriers) for demodulation, are unique communication systems using characteristics of chaos. However, the communication performance of the noncoherent system is lower as compared with the standard communication systems. Thus, it is important to advance noncoherent system in order to improve its performance. In our previous research, we have proposed a novel error-correcting method using a separation and reconstruction of the chaotic dynamics, which is one of characteristics of chaos. As simulation results, we have confirmed that the advantage gained in BER performance of our error-correcting method is about 2–2.5 dB compared to the conventional one (w/o coding). This paper focuses on a number of transmitting data and a combination of symbols, and analyzes an error-correcting capability for evaluating advantages of the separation and reconstruction of the chaotic dynamics in detail.

Key words Chaos, Noncoherent Chaos Communication, Error-Correcting Scheme, Chaotic Dynamics

1. まえがき

カオスは非周期的であり、理論的には無限周期の系列を生成する事ができる。また、極めてシンプルなモデルからもカオス

系列は生成可能であり、ダイナミクスと正確な初期値が与えられれば、指定した先の値を決定する事ができる。このような様々な特徴を活かして、現在、カオスを工学システムに応用する研究が盛んに行われている。特に、カオスを利用した通信シ

システムは、その代表的な応用の1つである [1]– [8]、中でも、カオス系列によって変調された信号のみを用いて復調を行うノンコヒーレントカオス通信システムは、カオスの特徴を活かした独特の通信システムとして知られている。ノンコヒーレントシステムを用いた手法としては、Differential chaos shift keying (DCSK) [1] と Optimal Receiver [2] が有名である。さらに、効率的なアルゴリズムを用いて、Optimal Receiver と同等もしくはそれに近い特性を有する Suboptimal receiver の開発も重要視されている [3]。しかしながら、これらのシステムではカオスの特徴を用いての変復調という制限があるため、一般的な通信システムと比較すると、通信特性は劣る事が知られている。ゆえに、ノンコヒーレント通信の特性向上のためには、カオスの特徴を利用したさらなる工夫が必要である。

私達はこれまでの研究で、ノンコヒーレントカオス通信システムのための、カオスダイナミクスに基づく誤り訂正手法を提案した [7]。一般的なカオス通信システムでは、送信機で1ビットのデータがある一定の長さのカオス系列で変調し、受信機でその長さごとに復調を行う。この時、受信機は、各データの変調に用いられたカオス系列のみを用いて復調を行っており、そのデータの前後のカオス系列は考慮していない。私達は、データの前後のカオス系列を同一のカオスダイナミクスにしたがって生成された連続するカオス系列として捉え、これをデータを正確に復調するための受信機への付加情報として誤り訂正に利用した。シミュレーションを行い、従来手法(誤り訂正無し)と比較した結果、ビット誤り率(BER)特性において、1~1.5 dB の利得を得る事を確認した。

さらに私達は、この誤り訂正手法を発展させ、カオスダイナミクスの分離を利用した誤り訂正手法を提案した [8]。今、 K 個の1ビットデータを、 K 個の信号ブロックとして伝送する場合を考える。本手法では、送信機側で信号ブロックの順序を故意に並び替え、信号ブロック間で連続するカオスダイナミクスを分離させる。この時、各ブロックが持つカオス系列の順序は入れ替えない。受信機側では、それを元に戻す動作(再構成)を行い、再構成した系列のカオスダイナミクスを解析する事によって誤り訂正を行う。つまり、カオスダイナミクスの分離と再構成を信号復調の際の付加情報として利用した誤り訂正手法である。先ほどと同様、シミュレーションを行った結果、従来手法(誤り訂正無し)と比較して、BER 特性において2~2.5 dB の利得を得る事ができた。

しかしながら、文献 [8] では、パラメータを限定した基礎的なシミュレーションしか行っていない。カオスダイナミクスの分離と再構成の効果を確認するためには、本手法の詳細な解析を行う必要がある。本稿では、シミュレーションパラメータとして、送信信号ブロック数(K)とその信号の組み合わせに注目し、文献 [8] で提案した手法の誤り訂正能力の解析を行う。

2. システムモデル

図1に、カオスダイナミクスの分離と再構成による誤り訂正手法を用いたCSK通信システムのブロック図を示す。詳しい動作については文献 [8] に記しており、本章では各ブロックの

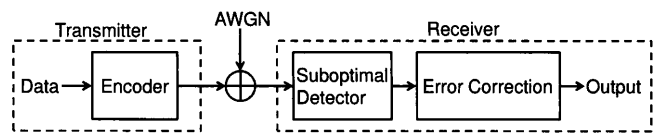


図1 カオスダイナミクスの分離と再構成による誤り訂正手法を用いたCSK通信システム。

Ex. $K=4$

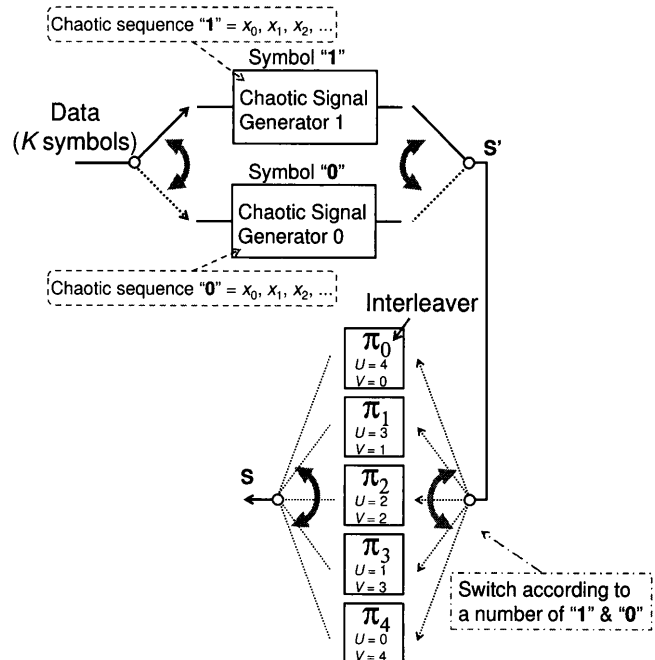


図2 送信機 (ex. $K = 4$).

動作について簡潔に説明する。

2.1 送信機

送信機では、1ビットデータをカオス写像によって生成されたカオス系列を用いて変調する。本研究では、カオス写像に、式(1)で表されるSkew Tent Mapを用いる。

$$x_{i+1} = \begin{cases} \frac{2x_i + 1 - a}{1 + a} & (-1 \leq x_i \leq a), \\ \frac{-2x_i + 1 + a}{1 - a} & (a < x_i \leq 1). \end{cases} \quad (1)$$

ここで、 $i = 0, 1, \dots, N-1$ 、 a は Skew Tent Map の頂点を表すパラメータである。本研究では、カオスを利用したデジタル変調方法として知られている、Chaos Shift Keying (CSK) を基に変調器を設計する。先に述べた通り、本誤り訂正手法では K 個の1ビットデータを、 K 個の信号ブロックとして伝送する ($K : 0, 1, \dots, j, \dots, K-1$)。図2に $K = 4$ と設定したときの送信機のモデルを示す。

まず、送信データにしたがって、カオス信号生成器(カオス写像)が選択され、1ビットデータに対し系列長 N のカオス系列が生成される。 K 個のデータが送信される時、データ量は $K \times N$ となる。つまり、提案手法の1ビットあたりのデータ量は、一般的なCSKシステムのそれと同じである。初期値は、信号ブロックを作る際ランダムに決定され、その値は各カオス信号生成器で異なる。加えて、 j 番目の系列の初期値は、1つ

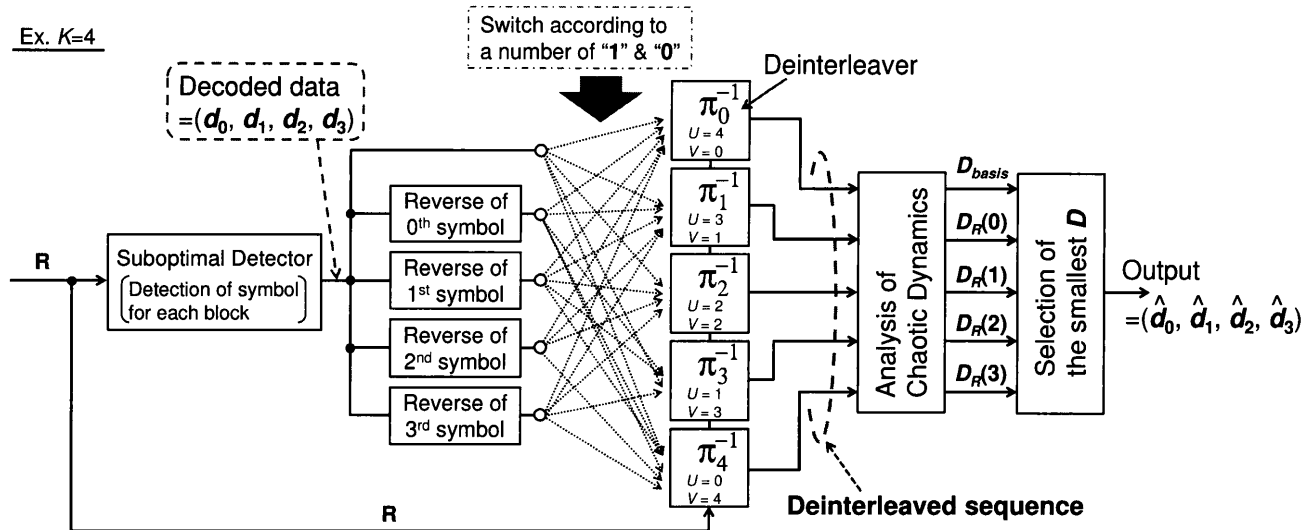


図3 受信機 (ex. $K = 4$).

前でおかつ j 番目のデータと同じデータの系列の最後の値から生成された値を使用する。この動作によって生成された系列を送信データの順にしたがって一繋ぎに接続し、この系列を信号ベクトル S' で表す。

この生成された系列 S' が持つカオスダイナミクスを分離させるため、信号ブロックの順序をインターリーブ π_k ($k : 0, 1, \dots, K$) を用いて入れ替える。事前に、 $K + 1$ 個のインターリーブを用意しておき、インターリーブが持つ系列入れ替えパターンは、送信データ “1” の総数 U 、 “0” の総数 V によって異なるように設定する。本研究では、各インターリーブの入れ替えパターンはランダムに決定する。ただし、各インターリーブのパターンと同一のパターンは他のインターリーブでは用いない。1章で述べた通り、本手法では信号ブロックのみを入れ替える。つまり、各信号ブロック内の系列の順序は変化しない事に注意する。インターリーブによって信号ブロックの順序を並べ替えられた系列を信号ベクトル S で表し、この系列が送信信号として受信機側に送られる。

2.2 伝送路

本研究では、伝送路でのノイズに相加性白色ガウス雑音 (additive white Gaussian noise: AWGN) を用いる。ゆえに、受信系列は、信号ベクトル $R = S + AWGN$ と表す事ができる。

2.3 受信機

受信機では、受信系列からデータの復調を行い、その後、誤り訂正を実行する。本研究では、ノンコヒーレントカオス通信システムを考えているため、受信機は送信機で用いたカオス写像を記録している。しかしながら、送信機側で生成したカオス系列の初期値は記録されていない。つまり、送受信機間で同一のカオス系列を生成する事はできない事を意味する。

図3に、 $K = 4$ に対する受信機を示す。まず初めに、受信機は、受信された系列を1ビットごと (長さ N ごと) に区切り、その区切られた各受信ブロックから、データをノンコヒーレント検出によって復調する。本手法では、ノンコヒーレント検出として、私達がこれまでに提案した Suboptimal 検出アルゴリ

ズムを用いる [7]。このアルゴリズムでは、送信機側で用いたカオス写像と受信ブロックとの最短距離を計算する事でデータの検出を行う。最短距離の計算は、受信ブロックが持つ N_d 個の連続する系列とカオス写像を N_d 次元スペースで表したもので行う ($N_d : 2, 3, \dots$)。本稿ではカオス写像に Skew Tent Map を用いており、これを N_d 次元スペースで表すと、そのスペース上に存在する直線の総数 l は $l = 2^{N_d - 1}$ となる。ゆえに、 l 本全ての直線との距離を計算し、その中から最も小さい距離を最短距離と決定する。角信号ブロックの系列長 N が、 N_d と等しい時 ($N = N_d$)、最短距離は1つだけ計算される。 N が N_d より大きい場合 ($N > N_d$)、系列の位置をずらして、再度最短距離を計算する (この時、系列の位置のずらしは $N - N_d$ 回行われる)。受信機は送信機側で用いた2種類の写像それぞれとの最短距離 $\sum D_1$ と $\sum D_0$ を計算し比較を行う。ここで、 $\sum D_1$ は送信データ “1” の写像、 $\sum D_0$ は送信データ “0” の写像との最短距離を表している。距離を比較した結果、 $\sum D_1 < \sum D_0$ であればデータ “1”、 $\sum D_1 > \sum D_0$ であればデータ “0” と判定する。

各受信ブロックごとのデータを復調後、受信機は誤り訂正を実行する。本稿では、 K 個の信号系列内の1ビットの訂正を考える。まず、受信機は復調されたデータに基づいて受信系列をソート、つまり、データ “1” と “0” の系列に分類する。さらに、受信機は復調されたデータ “1” と “0” の数をそれぞれ数え、デインターリーブ π_k^{-1} を選択する。デインターリーブは、送信機側のインターリーブによって並び替えられた系列を元に戻す (再構成) 動作を行う。ただし、送信されたデータ “1” と “0” の数と、復調されたそれとが一致した場合のみ、元の系列に戻す事ができるとする。本稿では、データ “1” のデインターリーブされた系列を M 、データ “0” のそれを N と仮定する。このデインターリーブされた系列 M と N のカオスダイナミクスを解析する。カオスダイナミクスの解析のため、本手法ではデータの復調に用いた Suboptimal 検出アルゴリズムを利用する。すなわち、カオス写像の N_d 次元スペースとデインターリーブさ

れた系列との最短距離を計算する。本稿では、復調されたデータにしたがってデインターリーブされた系列から計算される最短距離を、参照距離 D_{basis} と定義し、以下のように計算する。

$$D_{basis} = GoD_1(M) + GoD_0(N). \quad (2)$$

ここで、 $GoD_1(M)$ はデータ “1” の N_d 次元スペースと M との最短距離、 $GoD_0(N)$ はデータ “0” の N_d 次元スペースと N との最短距離をそれぞれ表している。

さらに受信機は、 j 番目のデータで誤りが生じたと仮定し、そのデータを反転させ、それに基づいて系列のソートを行う。そして、反転させたデータとそれ以外のデータにしたがってデインターリーブを選択する。このデインターリーブされた系列を用いて、 j 番目のデータを反転させた時の最短距離 $D_R(j)$ は以下のように計算される。

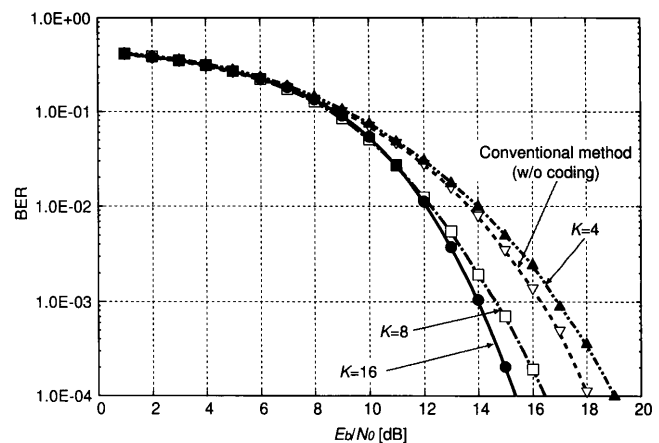
$$D_R(j) = GoD_1(M^{(j)}) + GoD_0(N^{(j)}). \quad (3)$$

ここで、 $M^{(j)}$ と $N^{(j)}$ は、 j 番目のデータを反転させた時の M と N をそれぞれ表している。

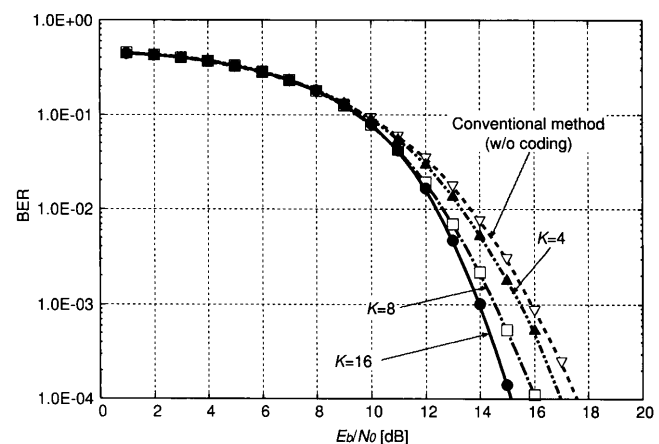
最後に受信機は、計算された全ての距離 (D_{basis} , $D_R(0)$, $D_R(1)$, \dots , $D_R(K-1)$) の中で最も小さい値を選び、それにしたがって誤り訂正を行う。もし受信機が、最初の Suboptimal 検出器で誤り無く復調できたとすると、 $D_R(j)$ は D_{basis} よりも大きな値となる。ゆえに、 D_{basis} が最も小さくなった場合は、最初に復調されたデータがそのまま出力される。一方、もし最初の Suboptimal 検出器で誤りが生じたとすると、 $D_R(0)$ から $D_R(K-1)$ の中のどれか1つが D_{basis} よりも小さな値となる。この時、最も小さな値となる $D_R(j)$ を選ぶ事で、 j 番目のデータの訂正を行う事ができる。

3. 誤り訂正能力の解析

1章で述べた通り、本稿では、送信信号ブロック数 (K) とその信号の組み合わせに注目して、2章で述べたカオスダイナミクスの分離と再構成による誤り訂正手法の誤り訂正能力の解析を行う。シミュレーション諸元を以下に記す。送信機側において、Skew Tent Map の頂点 a を 0.05、カオス系列長 N を 4 もしくは 8 とする。受信機側において、最短距離の計算のために、カオス写像の 4 次元スペース ($N_d = 4$) を用いる。送受信機で用いるインターリーブとデインターリーブの数はそれぞれ $K+1$ となり、並び替えパターンは事前にランダムに決めておく。また、 k 番のインターリーブ π_k で並び替えられた系列は、 k 番のデインターリーブ π_k^{-1} で元に戻るように、送受信機間で並び替えパターンの情報を共有していると仮定する。加えて、各インターリーブの並び替えパターンと同一のパターンは他のインターリーブで用いないように設定する。以上の諸元に基づき、本研究では 2 種類のシミュレーションを行う。一つ目は、データを 10^4 ビット送信し、 $K = 4, 8, 16$ に変化させた時の E_b/N_0 に対する BER を求める。二つ目は、同じくデータを 10^4 ビット送信し、 $K = 4$ 一定、送信データ “1” の総数 U 、 “0” の総数 V を任意の数に固定させた時の E_b/N_0 に対する BER を求める。なお、受信機で行う誤り訂正は 1 ビットの



(a) $N = 4$.



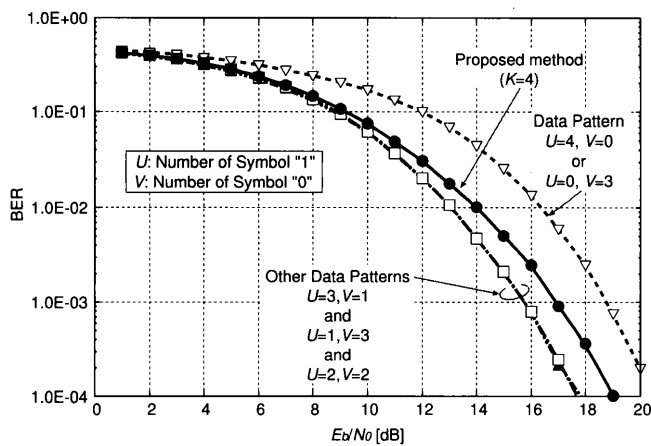
(b) $N = 8$.

図 4 BER vs. E_b/N_0 ($N_d = 4$).

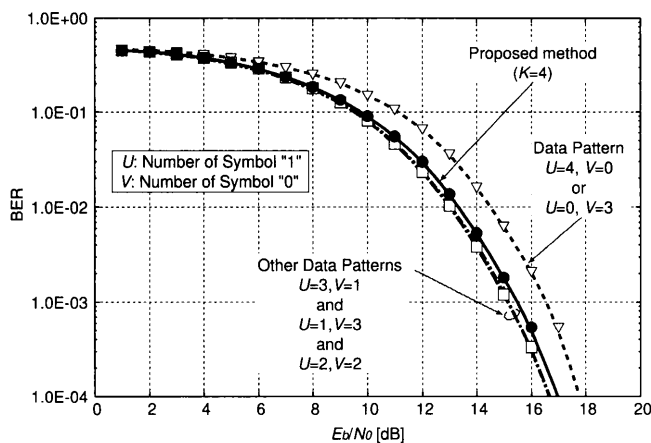
データの訂正のみと仮定する。

3.1 送信信号データ数 (K) に対する BER 特性

図 4(a) と (b) に、 N を一定、 $K = 4, 8, 16$ に変化させた時の E_b/N_0 に対する BER 特性の結果を示す (図 4(a): $N = 4$, (b): $N = 8$)。同図には比較のため、Suboptimal 検出アルゴリズムの BER 特性を従来手法 (誤り訂正無し) として表示している。結果から分かるように、送信信号データ数の変化に依存して、BER 特性が異なる事が確認できる。どちらの結果も、 $K = 16$ の時の誤り訂正手法の BER 特性が最も良い特性を示しており、従来手法と比較して約 2 ~ 2.5 dB の利得を得られている事が確認できる。特性が向上した理由として、インターリーブとデインターリーブによるカオスダイナミクスの分離・再構成が効果的に働いたためであると考えられる。一方で、 $K = 4$ の時は BER 特性はそれほど向上しておらず、 $N = 4$ の結果に至っては従来手法よりも特性が劣化してしまった。BER 特性の劣化はインターリーブとデインターリーブによる、カオスダイナミクスの分離・再構成が十分に行われていない事を意味している。これには、送信信号ブロック内のデータ “1” の総数 U 、 “0” の総数 V も大きく影響していると考えられる。この劣化の原因をより詳細に解析するため、次節では $K = 4$ 一定とした時の任意の送信データに対する BER 特性を調査する。



(a) $N = 4$.



(b) $N = 8$.

図5 任意の送信データに対する BER 特性 ($N_d = 4, K = 4$).

3.2 任意の送信データに対する BER 特性

図5(a)と(b)に、 $K = 4$ 一定、送信データ“1”の総数 U ，“0”の総数 V を任意の数に固定させた時の BER 特性を示す(図5(a): $N = 4$, (b): $N = 8$). $K = 4$ の時、送信信号ブロック内のデータ数は4であり、各データの総数は、(1) $U = 4, V = 0$ or $U = 0, V = 4$, (2) $U = 3, V = 1$ or $U = 1, V = 3$, (3) $U = 2, V = 2$, の3つのパターンに分ける事ができ、図5にはそれぞれのパターンの BER 特性を表示している。また、同図にはこれら3つの BER の平均値も表示している。これら2つの結果から分かるように、(1) $U = 4, V = 0$ or $U = 0, V = 4$ の BER 特性が、他のデータパターンよりもかけ離れた値を示している事が確認できる。 $U = 4$ 及び $V = 4$ は、送信信号ブロック内の全データが“1”もしくは“0”を意味しており、送信機では、どちらか一方のカオス写像のみを用いてカオス系列を生成する事となる。これは言い換えると、もう一方のカオス写像は用いられていない事となる。つまり、生成されたカオス系列には単一のカオス写像に基づくカオスダイナミクスのみが含まれ、もう一方のカオス写像に基づくダイナミクスは含まれない。これは、誤り訂正を行う際に必要となる付加情報が他のデータパターンよりも少ない事を意味する。ゆえに、本手法を用いて誤り訂正の効果を得るためには、送信データに応じた2つのカオス写像に基づく双方のダイナミクスを含んだ送信信号

を生成する必要があると考える。

4. むすび

本稿では、カオスダイナミクスの分離・再構成による誤り訂正手法の性能評価のため、送信信号ブロック数 (K) とその信号の組み合わせに注目した誤り訂正能力の解析を行った。シミュレーションを行った結果、カオスダイナミクスの分離・再構成による誤り訂正の効果を得るためには、 K を適切に設定し、さらに、送信データに応じた2つのカオス写像に基づく双方のダイナミクスを含んだ送信信号を生成する必要があるということが分かった。

文 献

- [1] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, “Differential chaos shift keying: A robust coding for chaos communication,” *Proc. NDES'96*, pp. 87-92, Jun. 1996.
- [2] M. Hasler and T. Schimming, “Chaos communication over noisy channels,” *Int. J. Bifurcation and Chaos*, vol. 10, no. 4, pp. 719-736, Apr. 2000.
- [3] M. Hasler and T. Schimming, “Optimal and suboptimal chaos receivers,” *Proc. IEEE*, vol. 90, Issue 5, pp. 733-746, May 2002.
- [4] W. M. Tam, F. C. M. Lau and C. K. Tse, *Digital Communications with Chaos*, Elsevier Science & Technology, 2006.
- [5] F. J. Escribano, S. Kozic, L. López, M. A. F. Sanjuán and M. Hasler, “Turbo-like structures for chaos encoding and decoding,” *IEEE Trans. Communications*, vol.57, no.3, pp.597-601, Mar. 2009.
- [6] G. Kaddoum and F. Gagnon, “Error correction codes for secure chaos-based communication system,” *Proc. QBSC'10*, pp. 193-196, May 2010.
- [7] S. Arai, Y. Nishio and T. Yamazato, “Error-Correcting Scheme Based on Chaotic Dynamics and its Performance for Noncoherent Chaos Communications,” *NOLTA, IEICE*, vol. 1, no. 1, pp. 196-206, Oct. 2010.
- [8] S. Arai, Y. Nishio and T. Yamazato, “Improvement of Error-Correcting Method Based on Chaotic Dynamics for Noncoherent Chaos Communications,” *Proc. NOLTA'12*, pp. 801-804, Oct. 2012.