2013 International Workshop on Nonlinear Circuits,
Communications and Signal Processing
NCSP'13, Israel of Hawaii, Hawaii, USA. March 4-7, 2013

# Performance Analysis of Error-Correcting Method Using Separation of Chaos for Noncoherent Chaos Communications

Shintaro Arai†, Yoshifumi Nishio‡ and Takaya Yamazato*

†Kagawa National College of Technology
551 Kohda, Takuma-cho, Mitoyo, Kagawa, JAPAN
Email: arai@cn.kagawa-nct.ac.jp

‡Tokushima University
2-1 Minami-Josanjima, Tokushima, JAPAN
Email: nishio@ee.tokushima-u.ac.jp

* Nagoya University
Furo-cho, Chikusa-ku, Nagoya, JAPAN
Email: yamazato@nagoya-u.jp

## Abstract

This paper analyzes the performance of the error-correcting method, which was proposed in the previous research, using the separation and the reconstruction of chaos for noncoherent chaos communications. Especially, we focus on a number of transmitting data and a combination of symbols (i.e., data pattern). We consider that the capability of the error correction depends on the number of data and the data pattern because the proposed method performs the error correction using successive data symbols. This study performs simulations for the number of data and the data pattern, and evaluates BER performance of the proposed method.

## 1. Introduction

Chaos communication system is an interesting topic in the field of engineering chaos [1]– [6]. Especially, many researchers have focused on the development of noncoherent detections which do not need to use basis signals (unmodulated carriers) for demodulation at a receiver. Differential chaos shift keying (DCSK) [1] and the optimal receiver [2] are well-known as typical noncoherent systems. Moreover, it is also important to develop a suboptimal receiver, which has a performance equivalent to or similar to the optimal receiver, using more efficient algorithms [3].

In our previous research, we focused on the chaotic dynamics and proposed the error-correcting method using the chaotic dynamics for noncoherent systems [7]. In our error-correcting method, two successive chaotic sequences are generated from the same chaotic map; the second sequence is generated with an initial value which is the last value of the first sequence. In this case, successive chaotic sequences having the same chaotic dynamics are created. This feature gives the receiver additional information to correctly recover the information data and thus improves the bit error performance of the receiver. As results of simulations, we have confirmed that the advantage gained in the bit error rate (BER) performance of our method is about 1–1.5 dB compared to a conventional method (w/o coding).

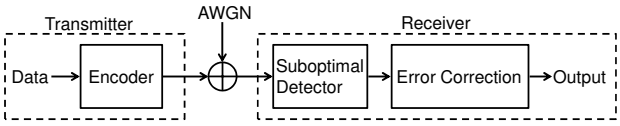


Figure 1: Block Diagram of CSK Communication System with Error-Correcting method.

Furthermore, we improved this method [7] using a separation and a reconstruction of the chaotic dynamics [8]. The method [7] uses the chaotic sequence generated according to the chaotic dynamics. In this case, it is very difficult to recover data without a successive sequence based on the chaotic dynamics. We focus on this feature and consider that an improved method separates and reconstructs the chaotic dynamics of the sequence according to a specific rule. As results of simulations, we have confirmed that the advantage gained in BER performance of our improved method is about 2–2.5 dB compared to the conventional one (w/o coding). However, we have only confirmed the performance of our method in primary simulations. In this paper, we focus on a number of transmitting data and a combination of symbols (i.e., data pattern), and analyze the performance of our method. It is considered that the capability of the error correction depends on the number of data and the data pattern because our method performs the error correction using successive data symbols. This study performs simulations for the number of data and the data pattern, and evaluates BER performance of our method.

## 2. Overview of Error-Correcting method [8]

This section briefly introduces the error-correcting method in [8]. We consider the discrete-time binary Chaos Shift Keying (CSK) communication system with the error correcting, as shown in Fig. 1.

### 2.1 Transmitter

In the transmitter, binary data are encoded by chaotic se-

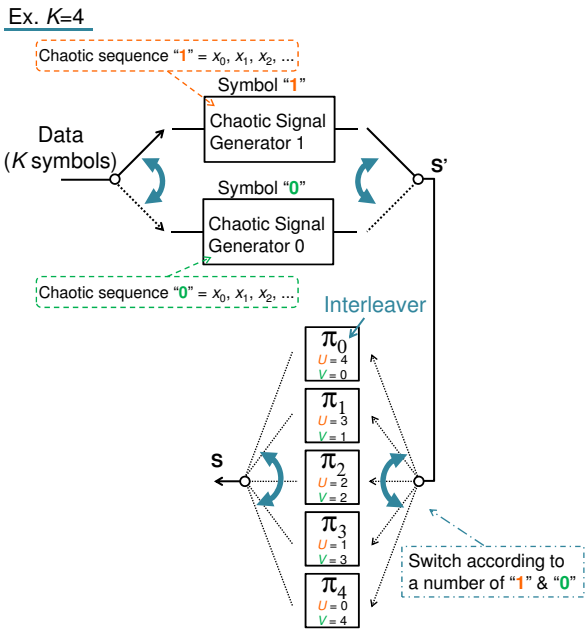


Figure 2: Operation of Encoder (ex. $K = 4$).

quences generated by a chaotic map. In this study, we use a skew tent map which is one of simple chaotic maps, and it is described as follows.

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

Where $i = 0, 1, \cdots, N-1$, $a$ denotes a position of the top of the skew tent map. Our encoder is designed based on CSK which is a digital modulation scheme using chaos. Figure 2 shows our encoder of the error-correcting method when $K = 4$, where $K$ denotes the number of transmitting data. To perform the error correction at the receiver, $K$ information bit are transmitted as $K$ signal blocks $(0, 1, \cdots, j, \cdots, K-1)$.

First, the encoder selects a chaotic signal generator according to the symbol and generates $N$ chaotic signal samples as a chaotic sequence, where $N$ denotes the chaotic sequence length. When $K$ bit data is transmitted, the amount of the data becomes $K \times N$. Thus, the amount of the data per bit of the proposed method becomes the same as the standard CSK. An initial value is chosen at random when beginning to make signal blocks and is different in each chaotic signal generator. In addition, the $j$-th sequence is generated from the initial value which is the end value of the former sequence with same symbol of $j$-th bit. The encoder connects each sequence according to the order of transmitting data and outputs the first signal vector $\mathbf{S}'$.

Next, the encoder shuffles the chaotic sequence in each symbol of $S'$ using an interleaver $\pi_k$ $(k : 0, 1, \cdots, K)$. Here, we explain conditions and operations of the interleaver. As an advance preparation, we prepare $K+1$ interleavers. Their shuffle patterns are different according to $U$ and $V$, where $U$ and $V$ denote the number of the transmitting symbol "1" and "0", respectively. Each interleaver's pattern is set at random and does not correspond with other one. In addition, the interleaver only shuffles the signal vector of each symbol. Note that the order of the sequence having each signal vector does not change. Therefore, the encoder shuffles the chaotic sequence in each symbol of $\mathbf{S}'$ according to the interleaver and outputs the second signal vector $\mathbf{S}$ as the transmitting sequence.

### 2.2 Channel

The channel distorts the signal and corrupts it by noise. In this study, noise of the channel is assumed to be the additive white Gaussian noise (AWGN). Thus, the received sequence vector $\mathbf{R}$ is given by $\mathbf{R} = \mathbf{S} + \text{AWGN}$.

### 2.3 Receiver

The receiver demodulates the information symbol from the received sequence. Also, the receiver performs the error correction in this study. Since we consider the noncoherent chaos communication, the receiver memorizes the chaotic map used for the modulation at the transmitter. However, the receiver never knows the initial value of chaos in the transmitter.

Our error-correcting method consists of the suboptimal detector and the error correction based on the chaotic dynamics, as shown in Fig. 3. First of all, the receiver performs the noncoherent detection for each received block and demodulates each symbol. In this study, we apply our suboptimal detection algorithm as the noncoherent detection [7, 8]. Our suboptimal detector calculates the shortest distance between $N_d$ samples of the sequence in each symbol and $N_d$-dimensional space made from $N_d$ successive chaotic signals generated by the skew tent map $(N_d : 2, 3, \cdots)$, and outputs the distance, which achieves the minimum shortest distance within the set of $l$. Where $l$ is the number of the straight lines in the $N_d$-dimensional space (i.e., $l = 2^{N_d - 1}$). When $N = N_d$, the receiver outputs one shortest distance. When $N > N_d$, the receiver shifts the extraction position for calculating the distance within $N$ signal samples and extracts $N_d$ samples from it. In this case, the number of the shift is $N - N_d$. The receiver calculates the shortest distance every extracting samples and outputs the sum of these shortest distances. When two symbols are transmitted, two kinds of the $N_d$-dimensional space corresponding to each symbol are made. The receiver calculates two shortest distances using two different $N_d$-dimensional space and outputs $\sum D_1$ and $\sum D_0$. Where $\sum D_1$ and $\sum D_0$ denote the sum of the shortest distance of the symbol "1" and "0", respectively. Finally, the receiver decides the decoded symbol as 1 (or 0) for $\sum D_1 < \sum D_0$ (or $\sum D_1 > \sum D_0$).

After demodulation of each symbol, the receiver performs the error correction. In this study, we consider the 1 bit correction in the proposed method. First, the receiver sorts the received sequence based on decoded symbols. In addition, the receiver counts the number of each decoded symbol and chooses a deinterleaver $\pi_k^{-1}$ corresponding to this number. The deinterleaver $\pi_k^{-1}$ reconstructs the sequence which is

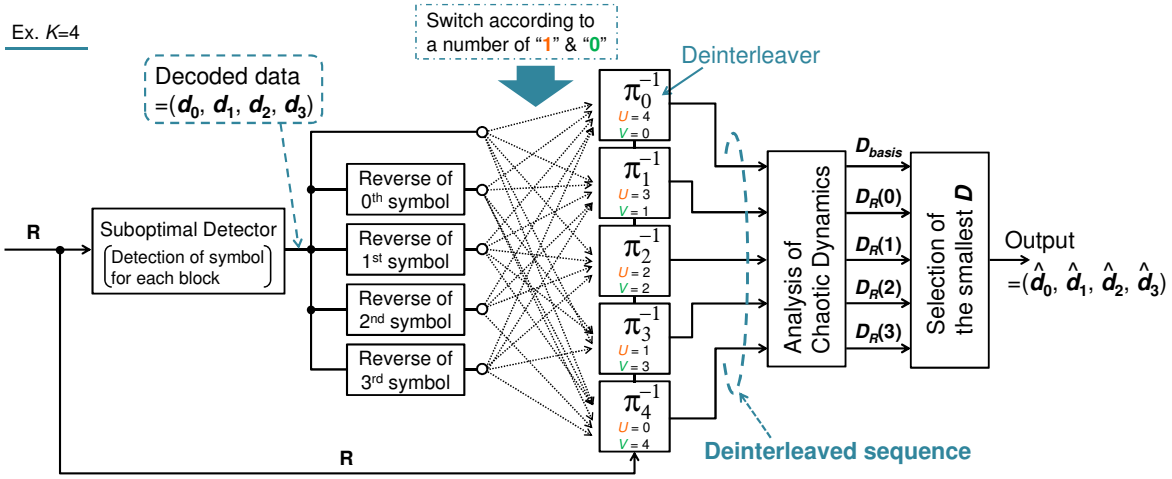


Figure 3: Proposed Error-Correcting Method [8] (ex. $K = 4$).

shuffled by the interleaver $\pi_k$ when the number of each symbol in the receiver corresponds with the transmitter one. Here, we define the deinterleaved sequence based on decoded symbol "1" and "0" as $\mathbf{M}$ and $\mathbf{N}$, respectively. Next, the receiver analyzes the chaotic dynamics of $\mathbf{M}$ and $\mathbf{N}$. For analyzing the chaotic dynamics, the receiver applies our suboptimal detection algorithm, i.e., the calculation of the shortest distance between the chaotic maps and two deinterleaved sequences. Thus, we define a reference distance $D_{basis}$ as follows.

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

Where $GoD_1(\mathbf{M})$ (or $GoD_0(\mathbf{N})$) is the shortest distance between $\mathbf{M}$ (or $\mathbf{N}$) and the $N_d$-dimensional space of the symbol "1" (or "0").

Next, the receiver assumes the detection error has occurred at the $j$-th symbol and reverses this symbol. Moreover, the receiver sorts the received sequence and chooses the deinterleaver according to the reversed symbol and other symbols. Using the deinterleaved sequence, we calculate the distance $D_R(j)$ as follows.

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

Where $\mathbf{M}^{(j)}$ and $\mathbf{N}^{(j)}$ denote deinterleaved sequences when the $j$-th decoded symbol is reversed. Here, $D_R(j)$ means the shortest distance between the deinterleaved sequence and the chaotic map corresponding to their sequences. If the receiver can detects symbols and deinterleaves the sequence correctly in the first step, $D_R(j)$ becomes lager values as compared with $D_{basis}$. On the other hands, if the error has occurred, some one of $D_R(0)$–$D_R(K-1)$ becomes smaller as compared with $D_{basis}$. Therefore, the receiver selects the smallest distance from $D_{basis}$ and $D_R(j)$ and corrects the error.

## 3. Performance Analysis

As described in Introduction, this paper focuses on the number of transmitting data (i.e., $K$) and the combination of symbols (i.e., data pattern), and analyzes the performance of the proposed error-correcting method in [8]. We consider that the capability of the error correction depends on the number of data and the data pattern because our method performs the error correction using successive data symbols. In this section, we perform the computer simulation of the error correction with following conditions and observe the influence of the number of data and the data pattern.

The simulation conditions are as follows. In the transmitting side, we assume $N = 4$. The parameter of the skew tent map is fixed as $a = 0.05$. For calculation of the shortest distance, we use 4-dimensional space ($N_d = 4$). In this study, we perform two kind of simulations. First is the simulation for the number of data $K$. Second is the simulation for the transmitting data pattern. In each simulation, we iterate the simulation 10,000 times and record BER for various $E_b/N_0$.

### 3.1 BER for Number of Data $K$

We show two kind of results for $K$. First, Fig. 4 shows BERs versus $E_b/N_0$ for different $K$ when $N = N_d = 4$. In Fig. 4, we plot the performance of the proposed method with $K = 4, 8, 16$ and 32 and the conventional one (w/o coding). Second, Fig. 5 shows BERs versus $K$ for different $E_b/N_0$. In Fig. 5, we plot the performance of the proposed one and the conventional one when $E_b/N_0$ =16dB, 14dB and 12dB. From these figures, we can confirm that BER performance of the proposed method improves as compared with the conventional one when $K \geq 8$. Especially, When $K = 16$, the advantage gained in BER performance of the proposed one is about 2–2.5 dB compared to the conventional one. However, we can also confirm that the performance of the proposed method gradually degrades with increasing $K$ when $K > 16$. This is because that the deinterleaved sequence length increases depending on large $K$. We consider that it becomes difficult to analyze the difference of the chaotic dynamics between symbols due to increasing of the deinterleaved sequence length. Next, let us focus on the performance of $K = 4$. As one can see, the performance of the conventional method is better than the proposed one when $K = 4$. This is because that the data pattern becomes small with de-

creasing $K$. We further discuss the performance for the data pattern in Sec. 3.2.

### 3.2 BER for Data Pattern

Figure 6 shows BERs versus $E_b/N_0$ for the different data pattern when $N = N_d = K = 4$. In the case of $K = 4$, there are three data patterns: 1) All symbols "1" or "0", 2) $U = 3$, $V = 1$ or $U = 1$, $V = 3$, 3) $U = V = 2$. As one can see, the performance of all symbols "1" or "0" degrades as compared with other performances. This reduction of the performance means the failure of the reconstruction of the chaotic dynamics in the deinterleaver $\pi_k^{-1}$. When we send the same data only, the encoder only uses one of chaotic maps. In this case, the transmitting sequence does not contain the chaotic dynamics (i.e., the additional information for the error correction) based on the another map. Therefore, the proposed error correction requires the transmitting sequence which contains the chaotic dynamics of both symbols.

## 4. Conclusions

This paper has focused on the transmitting data and has analyzed the performance of the proposed error-correcting method for the number of data and the data pattern. As analysis results, we have observed that it becomes difficult to analyze the difference of the chaotic dynamics between symbols due to increasing of the number of the transmitting data. In addition, we have found that the proposed error correction requires the transmitting sequence which contains the chaotic dynamics of both symbols.

## References


[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] P. Stavroulakis, *Chaos Applications in Telecommunications*, Talor & Francis Group, 2006.

[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.


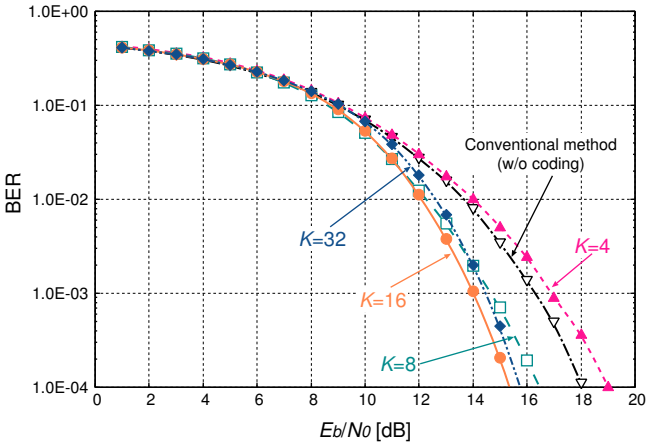


Figure 4: BER vs. $E_b/N_0$ for $K$ ($N = N_d = 4$).

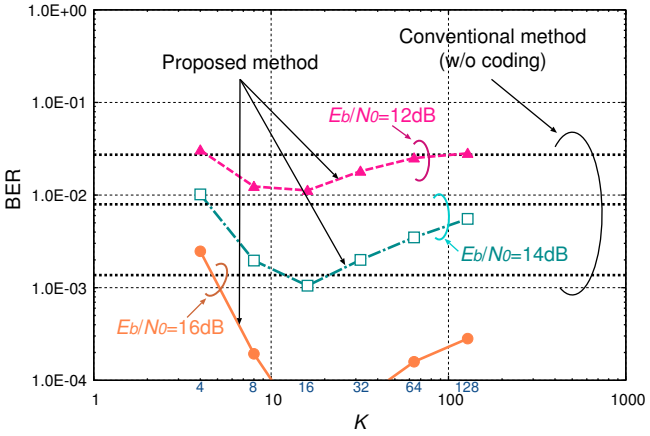


Figure 5: BER vs. $K$ ($N = N_d = 4$).

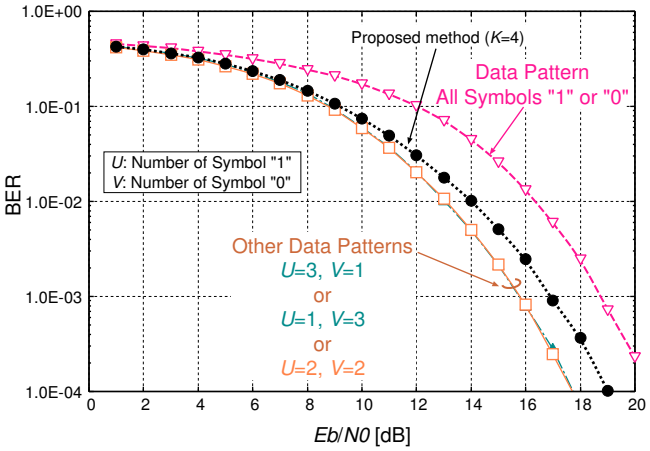


Figure 6: BER vs. $E_b/N_0$ for Data Pattern ($N = N_d = K = 4$).