2012 International Symposium on Nonlinear Theory and its Applications
NOLTA2012, Palma, Majorca, Spain, October 22-26, 2012

# Improvement of Error-Correcting Method Based on Chaotic Dynamics for Noncoherent Chaos Communications

Shintaro ARAI†, Yoshifumi NISHIO‡ and Takaya YAMAZATO††

†Dept. of Communication Network Engineering, Kagawa National College of Technology
551 Kohda, Takuma-cho, Mitoyo, Kagawa 769-1192, JAPAN
‡Dept. of Electrical and Electronic Engineering, Tokushima University
2-1 Minami-Josanjima, Tokushima 770-8506 JAPAN
††Institute of Liberal Arts and Science, Nagoya University
Furo-cho, Chikusa-ku, Nagoya 464-8063 JAPAN
Email: arai@cn.kagawa-nct.ac.jp, nishio@ee.tokushima-u.ac.jp, yamazato@nagoya-u.ac.jp

**Abstract**—This paper focuses on characteristics of the chaotic dynamics and improves our previous error-correcting method using them for noncoherent chaos communications. Our previous method is performed by using a 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. Namely, the separation and reconstruction of the chaotic dynamics can be applied for our improved method as additional information. 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 a conventional method (without coding).

## 1. Introduction

Chaos communication system is an interesting topic in the field of engineering chaos [1]– [5]. 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 [6]. 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. Further, our method is operated without a redundancy bit sequence referred to perform an error correction in standard communication systems. As results of computer simulations, we 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 (without coding). Moreover, we found that the chaotic dynamics had a great influence on the demodulation of chaos communications.

In this study, we further focus on the characteristics of the chaotic dynamics and improve our error-correcting method using them. Our error-correcting method is performed by using a 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 consider that the chaotic dynamics of the sequence is purposely separated using a specific rule. A transmitter shuffles the order of the sequence according to the specific rule for separating the chaotic dynamics, and a receiver reconstructs the original chaotic sequence using the same rule. Namely, the separation and reconstruction of the chaotic dynamics can be applied for our error-correcting method as additional information. In this paper, we describe operations of our improved error-correcting method. In addition, we carry out computer simulations and evaluate BER performance of the improved method.

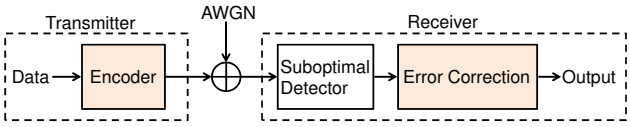



Figure 1: Block Diagram of CSK Communication System with Error-Correcting method.

## 2. System Overview

We consider the discrete-time binary Chaos Shift Keying (CSK) communication system with the error correcting, as shown in Fig. 1. Detail of each block is described below.

### 2.1. Transmitter

In the transmitter, binary data are encoded by chaotic sequences 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.

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

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 us-

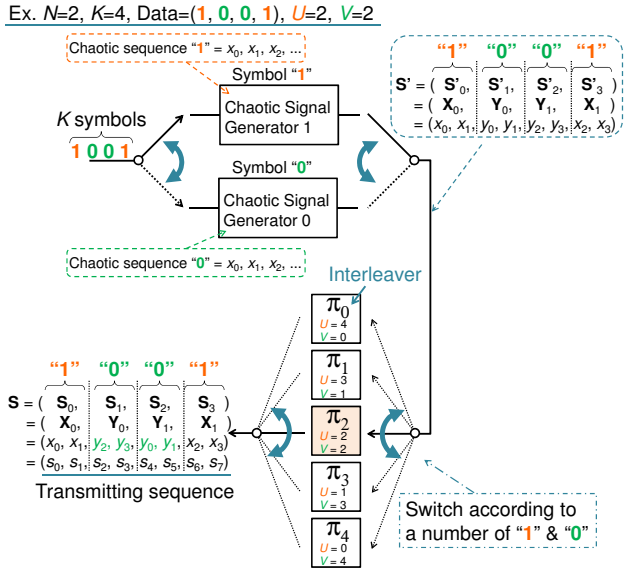



Figure 2: Operation of Encoder (ex. $N = 2$, $K = 4$).

ing chaos. Figure 2 shows our encoder for our error-correcting method. To perform the error correction at the receiver, $K$ information bit are transmitted as $K$ signal blocks $(0, 1, \cdots, j, \cdots, K-1)$. The encoder selects a chaotic signal generator according to the symbol. Here, we denote "$f^{(i)}(x_0)$" as the skew tent map (Eq. (1)). When the symbol "1" and "0" are sent, $f^{(i)}(x_0)$ and $g^{(i)}(x_0)$ $(= -f^{(i)}(x_0))$ are used, respectively. Also, we denote $U$ and $V$ as a total number of symbol "1" and "0", respectively. Thus, the signal vector $\mathbf{X}_u$ and $\mathbf{Y}_v$ are different for each symbol.

**When the symbol "1" is sent,**

$$\mathbf{X}_u = (x_j,\ f^{(1)}(x_j), \cdots, f^{(i)}(x_j), \cdots, f^{(N-1)}(x_j)). \tag{2}$$

**When the symbol "0" is sent,**

$$\mathbf{Y}_v = (y_j,\ g^{(1)}(y_j), \cdots, g^{(i)}(y_j), \cdots, g^{(N-1)}(y_j)). \tag{3}$$

Where $u = 0, 1, \cdots, U-1$, $v = 0, 1, \cdots, V-1$, $x_j$ or $y_j$ denotes the initial value of the $j$th symbol = "1" or "0" respectively, $N$ is the chaotic sequence length per 1 bit. 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. As an example, we assume $N = 2$, $K = 4$ and the data are (1, 0, 0, 1), as shown in Fig. 2. In this case, the signal vector $\mathbf{S}'(= \mathbf{S}'_0, \mathbf{S}'_1, \cdots, \mathbf{S}'_{K-1})$ is given as follows.

$$\begin{aligned} \mathbf{S}' &= (\mathbf{S}'_0, \mathbf{S}'_1, \mathbf{S}'_2, \mathbf{S}'_3) = (\mathbf{X}_0, \mathbf{Y}_0, \mathbf{Y}_1, \mathbf{X}_1) \\ &= (x_0, x_1, y_0, y_1, y_2, y_3, x_2, x_3). \end{aligned}$$

As one can see, the initial value of the 3rd symbol ($\mathbf{S}'_3$) and 2nd symbol ($\mathbf{S}'_2$) is generated by the end value of 0th symbol ($\mathbf{S}'_0$) and 1st symbol ($\mathbf{S}'_1$), respectively.

In this study, the encoder shuffles the chaotic sequence in each symbol 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. These shuffle patterns are different according to the number of each transmitting symbol. 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. For example, Tab. 1 shows the patterns of the interleaver when $K = 4$. The encoder counts the number of each symbol and chooses the interleaver corresponding to this number. In the case of data=(1, 0, 0, 1), $\pi_2$ is chosen because the number of the symbol "1" and "0" is two respectively. Therefore, the transmitting sequence $\mathbf{S}(= \mathbf{S}_0, \mathbf{S}_1, \cdots, \mathbf{S}_{K-1})$ is given as follows.

$$\begin{aligned} \mathbf{S} &= (\mathbf{S}_0, \mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3) = (\mathbf{X}_0, \mathbf{Y}_1, \mathbf{Y}_0, \mathbf{X}_1) \\ &= (x_0, x_1, y_2, y_3, y_0, y_1, x_2, x_3) \\ &= (s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7). \end{aligned} \tag{4}$$

As one can see, $\mathbf{Y}_0$ switches positions with $\mathbf{Y}_1$ according to $\pi_2$.

Table 1: Example Pattern of Interleaver ($\pi_k$): $K = 4$.

| | Number of each symbol | Before | After |
|---|---|---|---|
| $\pi_0$ | $U = 4$ | $\mathbf{X}_0, \mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$ | $\mathbf{X}_1, \mathbf{X}_3, \mathbf{X}_0, \mathbf{X}_2$ |
| | $V = 0$ | – | – |
| $\pi_1$ | $U = 3$ | $\mathbf{X}_0, \mathbf{X}_1, \mathbf{X}_2$ | $\mathbf{X}_1, \mathbf{X}_0, \mathbf{X}_2$ |
| | $V = 1$ | $\mathbf{Y}_0$ | $\mathbf{Y}_0$ |
| $\pi_2$ | $U = 2$ | $\mathbf{X}_0, \mathbf{X}_1$ | $\mathbf{X}_0, \mathbf{X}_1$ |
| | $V = 2$ | $\mathbf{Y}_0, \mathbf{Y}_1$ | $\mathbf{Y}_1, \mathbf{Y}_0$ |
| $\pi_3$ | $U = 1$ | $\mathbf{X}_0$ | $\mathbf{X}_0$ |
| | $V = 3$ | $\mathbf{Y}_0, \mathbf{Y}_1, \mathbf{Y}_2$ | $\mathbf{Y}_0, \mathbf{Y}_2, \mathbf{Y}_1$ |
| $\pi_4$ | $U = 0$ | – | – |
| | $V = 4$ | $\mathbf{Y}_0, \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Y}_3$ | $\mathbf{Y}_2, \mathbf{Y}_0, \mathbf{Y}_3, \mathbf{Y}_1$ |

## 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 is given by $\mathbf{R} = (r_0,\ r_1, \cdots,\ r_{KN-1}) = \mathbf{S} +$ 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. In the next section, we describe operations of our improved error-correcting method in detail.

# 3. Improved Error-Correcting method

Our error-correcting method consists of the suboptimal detector and the error correction based on chaotic dynamics, as shown in Fig. 3.

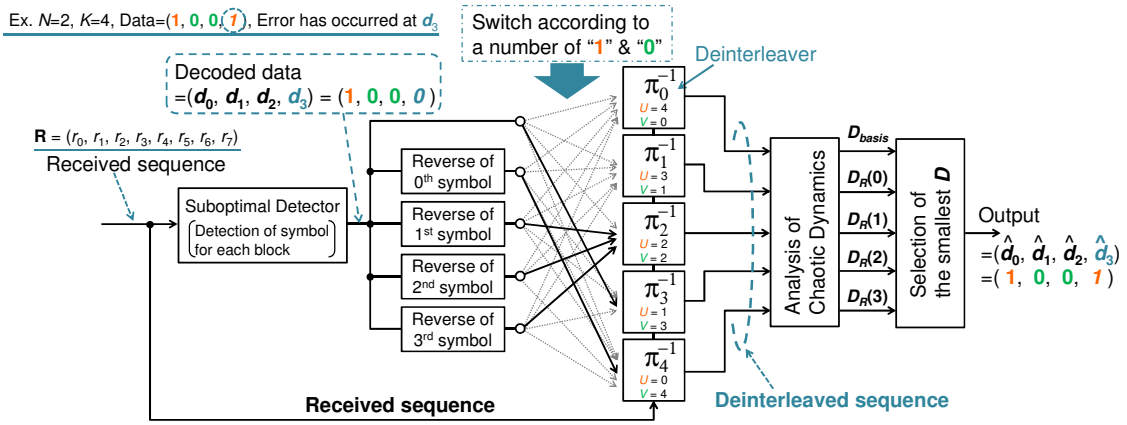



Figure 3: Operation of Improved Error-Correcting Method (ex. $N = 2$, $K = 4$).

First, 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 [6]. Our suboptimal detector calculates the shortest distance between $\mathbf{R}'_i$ 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 sum of the distance, which achieves the minimum shortest distance within the set of $l$, from $i = 0$ to $N - N_d$. Here, $\mathbf{R}'_i$ is the $N_d$ successive signals beginning with $i$ with in the received signals defined as

$$\mathbf{R}'_i = (r_{\alpha+i}, r_{\alpha+i+1}, ..., r_{\alpha+i+N_d-1}), \quad (5)$$

where $\alpha = j \times N$. Also, $l$ is the number of the straight lines in the $N_d$-dimensional space (i.e., $l = 2^{N_d-1}$). When two symbols are transmitted, two kinds of the $N_d$-dimensional space corresponding to each symbol are made. Let us consider the case of Symbol "1". For calculating the shortest distance, we find the closest point $\mathbf{P}_l$ between $\mathbf{R}'_i$ and the $l$-th line using the scalar product of the vector. When both edges of the $l$-th line are defined as $\mathbf{P}'_l$ and $\mathbf{P}''_l$, as shown in Fig. 4, the closest point $\mathbf{P}_l$ is calculated by the following equation.

$$\mathbf{P}_l = (\mathbf{u}_l \cdot \mathbf{v}_l)\,\mathbf{u}_l + \mathbf{P}'_l, \quad (6)$$

$$\text{unit vector } \mathbf{u}_l = \frac{\mathbf{P}''_l - \mathbf{P}'_l}{||\mathbf{P}''_l - \mathbf{P}'_l||}, \quad (7)$$

$$\mathbf{v}_l = \mathbf{R}'_i - \mathbf{P}'_l. \quad (8)$$

In the same ways, we can find the closest point $\mathbf{Q}_l$ between $\mathbf{R}'_i$ and the $l$-th line of the space of Symbol "0". Then, the above operations are expressed as

$$\sum D_1 = \sum_{i=0}^{N-N_d} \min_l ||\mathbf{P}_l - \mathbf{R}'_i||. \quad (9)$$

$$\sum D_0 = \sum_{i=0}^{N-N_d} \min_l ||\mathbf{Q}_l - \mathbf{R}'_i||. \quad (10)$$

Finally, we decide 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. For ease of explanation, we use same assumption in the explanation of the encoder (Fig. 2). Also, we assume that the detection error has occurred at the 3rd symbol ($d_3$), namely the case of 1 bit correction.

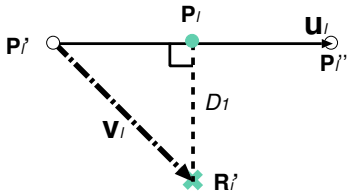



Figure 4: Calculation of Shortest Distance.

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 shuffled by the interleaver $\pi_k$ when the number of each symbol in the receiver corresponds with the transmitter one. In this example, $\pi_3^{-1}$ is chosen because the numbers of "1" and "0" are one and three, respectively. Here, we define the deinterleaved sequence based on decoded symbol "1" (or "0") as $\mathbf{M} = (m_0, m_1, \cdots, m_{C_1-1})$ (or $\mathbf{N} = (n_0, n_1, \cdots, n_{C_0-1})$), where $C_1$ and $C_0$ are the total of $\mathbf{M}$ 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.

$$D_{basis} = GoD_1(\mathbf{M}) + GoD_0(\mathbf{N}). \quad (11)$$

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 Symbol "1" (or "0").

$$GoD_1(\mathbf{M}) = \sum_{i=0}^{C_1-N_d} \min_l ||\mathbf{P}_l - \mathbf{M}'_i||. \quad (12)$$

$$GoD_0(\mathbf{N}) = \sum_{i=0}^{C_0-N_d} \min_l ||\mathbf{Q}_l - \mathbf{N}'_i||. \quad (13)$$

Next, the receiver assumes the detection error has occurred at the $j$-th symbol and reverses this symbol, as shown in Fig. 5. Moreover, the receiver sorts the received sequence and chooses the deinterleaver according to the re-

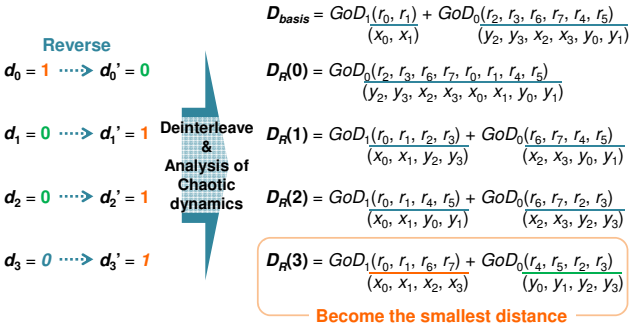



Figure 5: Calculation of $D_R(j)$ and Selection of the smallest distance.

versed symbol and other symbols. Using the deinterleaved sequence, we calculate the distance $D_R(j)$ as follows.

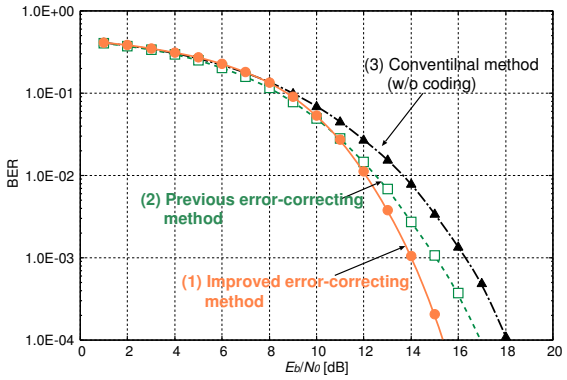
$$D_R(j) = GoD_1(\mathbf{M}^{(j)}) + GoD_0(\mathbf{N}^{(j)}). \quad (14)$$

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 $D_{basis}$. For instance, we consider that the error has occurred at the 3rd symbol, as shown in Fig. 5. In this case, $D_R(3)$ becomes the smallest distance as compared with $D_{basis}$ and other $D_R(j)$. The reason for this is that the receiver can reconstruct the original chaotic sequences of symbol "1" and "0" from the received sequence by choosing the correct deinterleaver. Therefore, the receiver selects the smallest distance from $D_{basis}$ and $D_R(j)$ and corrects an error. Additionally, in this example, the receiver can determine that the error has occurred at the 3rd symbol.

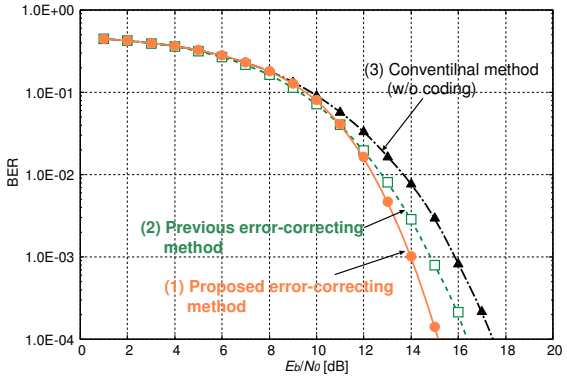
## 4. Simulation Results

We evaluate the performance of the improved error-correcting method by computer simulations. The simulation conditions are as follows. In the transmitting side, we assume $K = 16$. The parameter of the skew tent map is fixed as $a = 0.05$. For calculation of the shortest distance, we use 4-dimensional space ($N_d = 4$). Moreover, we only perform the 1 bit error correction. Based on these conditions, we iterate the simulation 10,000 times and calculate BER performance.

Figures 6(a) and (b) show the BERs versus $E_b/N_0$ for $N = 4$ and $N = 8$, respectively. We plot three performances: (1) Improved error-correcting method, (2) the previous one [6], (3) the conventional method (without coding). From these figures, we can confirm that the advantage gained in BER performance of the improved error-correcting method is about 2–2.5 dB compared to the conventional method. Moreover, it can be observed that the performance of the improved error-correcting method is better than the previous one. Namely, we achieve that the capability of our error-correcting method increases by separating and reconstructing the chaotic dynamics using the interleaver and the deinterleaver.




(a) $N = 4$.




(b) $N = 8$.

Figure 6: BER vs. $E_b/N_0$ ($K = 16$ and $N_d = 4$).

## 5. Conclusions

In this study, we have improved our proposed error-correcting method by separating the chaotic dynamics. As results, it has been achieved that the capability of the improved error-correcting method increases as compared with the previous one. Therefore, we have concluded that the separation and reconstruction of the chaotic dynamics are very effective as additional information to recover data.

## 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] J. C. Fang and C. K. Tse, *Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications*, Tsinghua University Press and World Scientific Publishing Co. Pte. Ltd., 2008.

[5] G. Kaddoum and F. Gagnon, "Error correction codes for secure chaos-based communication system," *Proc. QBSC'10*, pp. 193-196, May 2010.

[6] 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.