Chaos MIMO system with efficient use of information of bits

Ryo Yamazaki¹a), Yutaka Shimada², and Tohru Ikeguchi¹,³

¹ Department of Management Science, Graduate School of Engineering, Tokyo University of Science, Niijuku 6-3-1, Katsushika-ku, Tokyo 125-8585, Japan
² Department of Information and Computer Sciences, Graduate School of Science and Engineering, Saitama University, Shimo-Okubo 255, Sakura-ku, Saitama-shi, Saitama 338-8570, Japan
³ Department of Information and Computer Technology, Faculty of Engineering, Tokyo University of Science, Niijuku 6-3-1, Katsushika-ku, Tokyo 125-8585, Japan

a) yamazaki@hisenkei.net

Received January 31, 2020; Revised May 25, 2020; Published October 1, 2020

Abstract: The multiple-input multiple-output (MIMO) system is one of the wireless communication methods that use multiple transmit and receive antennas. To ensure security on the physical layer and also to enhance channel coding efficiency, a chaos MIMO (C-MIMO) system was previously proposed. In this system, a chaotic dynamical system is used for modulation. In this paper, we revealed that the original C-MIMO system does not effectively use the information of bits that are used for modulation, which results in a difficulty in distinguishing encrypted symbols. To solve this issue, we propose a new modulation method for the C-MIMO system. We evaluated the performance of the proposed C-MIMO system and showed that the proposed C-MIMO system significantly improves block error rates.

Key Words: chaos communication, MIMO, Bernoulli shift map

1. Introduction

Owing to the widespread use of the Internet, the development of high capacity and secure communication systems is required. To deal with this problem, it is acknowledged that the multiple-input multiple-output (MIMO) system [1] is effective owing to its large channel capacity. The MIMO system has already played an essential role in the fourth generation of cellular mobile communications (4G) and the fifth generation of cellular mobile communications (5G). Although the current MIMO system provides security for the layers higher than the physical layer, the security of the physical layer is not taken into consideration. However, as the number of users increases, the security of the current MIMO system is insufficient and encryption in the physical layer should be considered.

To ensure the security of the physical layer, the chaos-based communication method [2] is effective.
One of the well-known chaos-based communication methods is chaotic code division multiple access (C-CDMA) [3], where a chaos-based modulation is incorporated into the code division multiple access (CDMA); the C-CDMA ensures the security of the physical layer. However, the CDMA was not included in the 4G and 5G standards. Conversely, Okamoto et al. proposed a chaos MIMO (C-MIMO) system that ensures the security of the physical layer and also obtains channel coding gain by introducing a chaotic dynamical system in the signal modulation part [4–6]. The C-MIMO system is one of the common key cryptosystems, which uses the feature of chaotic dynamics such as a sensitive dependence on initial conditions. Although the original C-MIMO system shows high performance, it is still important to reveal why the chaotic dynamics leads to good performance from the perspective of nonlinear dynamical systems.

In this study, we numerically analyzed the dynamics of the chaotic system used in the modulation part of the original C-MIMO system [4–6] and clarified that there is a possibility that the original C-MIMO system [4–6] does not take full advantage of the information of bits used for signal modulation. Then, we further proposed a chaos-based modulation method for the modulation part in [6] and showed that the proposed C-MIMO system improves bit error rate (BER) and block error rate (BLER) performances, because the proposed C-MIMO system can effectively use the information of bits.

2. Chaos MIMO system

![Fig. 1. Original chaos multi-input multi-output (C-MIMO) system [4–6].](image)

In this section, we review a configuration of the original C-MIMO system [4–6]. Figure 1 shows the configuration of the original C-MIMO system.

Let \( N_t \) be the number of transmit antennas and \( N_r \) be the number of receive antennas. Figure 1 shows an example when \( N_t = N_r = 2 \). Let \( \mathbf{b} \) be a transmit block which is given by

\[
\mathbf{b} = [b_0, b_1, \cdots, b_{L-1}],
\]

where \( L \) is the number of symbols.

Let \( \mathbf{s}(t) \) be the \( t \) th MIMO transmit vector which is given by

\[
\mathbf{s}(t) = [s_1(t), \cdots, s_{N_i}(t)]^T,
\]

where \( s_i(t) (i = 1, \cdots, N_i) \) corresponds to the \( t \) th symbol transmitted from the \( i \) th transmit antenna and \( T \) represents the transpose. In Eq. (2), \( t \) represents the temporal order with which \( \mathbf{s}(t) \) is transmitted from the transmit antennas. The transmitted symbol \( s_i(t) \) is generated from the transmit block \( \mathbf{b} \) by the chaos-based modulation, which is described later in this section. Let \( \mathbf{S}_B \) be the MIMO transmit block consisting of \( B \) MIMO transmit vectors defined by

\[
\mathbf{S}_B = [\mathbf{s}(0), \cdots, \mathbf{s}(B-1)].
\]

Note that \( L = N_i B \). Then, the \( t \) th MIMO receive vector is given by

\[
\mathbf{r}(t) = \mathbf{H}(t)\mathbf{s}(t) + \mathbf{n}(t),
\]
where \( \mathbf{n}(t) \) is the \( t \)th noise vector whose elements obey the zero-mean Gaussian distribution. The matrix \( \mathbf{H}(t) \) is the \( t \)th channel matrix given by

\[
\mathbf{H}(t) = \begin{bmatrix}
    h_{11}(t) & \cdots & h_{1N_t}(t) \\
    \vdots & \ddots & \vdots \\
    h_{N_r,1}(t) & \cdots & h_{N_r,N_t}(t)
\end{bmatrix},
\]

(5)

where \( h_{ij}(t) \) is the \( t \)th channel component between the \( i \)th transmit antenna and the \( j \)th receive antenna. Values of \( h_{ij}(t) \) follow antenna and symbol independent and identically distributed (i.i.d.) flat Rayleigh fading. In the receiver, the transmit block \( \mathbf{b} \) is estimated from \( \mathbf{r}(t) \).

In the original C-MIMO system, a common key \( c_0 \) (\( 0 < \text{Re}[c_0] < 1 \) and \( 0 < \text{Im}[c_0] < 1 \)) is randomly generated and shared between the transmitter and the receiver in advance. The value of \( c_0 \) is used to generate the initial values of the chaotic dynamical systems. Figure 2 shows a configuration of the chaos modulation part [4–6].

![Fig. 2. Configuration of the chaos modulation part in the original C-MIMO system [4–6].](image)

The original C-MIMO system generates the MIMO transmit block \( \mathbf{S}_B \) by using a transmit block \( \mathbf{b} \) and the \( k \)th element symbol represented by \( c_k \) (\( k = 1, \cdots, L \)). The element symbol \( c_k \) is generated from \( c_0 \) by a chaos-based modulation described in the following procedure.

(I) Set \( k \) to 0.

(II) Two initial values of chaotic dynamical systems, \( x_0 \) and \( y_0 \), are generated from the element symbol \( c_k \) and the transmit block \( \mathbf{b} \) as follows:

\[
x_0 = \begin{cases} 
    \text{Re}[c_k] & (b_k = 0), \\
    1 - \text{Re}[c_k] & (b_k = 1 \text{ and } \text{Re}[c_k] > 1/2), \\
    \text{Re}[c_k] + 1/2 & (b_k = 1 \text{ and } \text{Re}[c_k] \leq 1/2),
\end{cases}
\]

and

\[
y_0 = \begin{cases} 
    \text{Im}[c_k] & (b_{(k+1) \mod L} = 0), \\
    1 - \text{Im}[c_k] & (b_{(k+1) \mod L} = 1 \text{ and } \text{Im}[c_k] > 1/2), \\
    \text{Im}[c_k] + 1/2 & (b_{(k+1) \mod L} = 1 \text{ and } \text{Im}[c_k] \leq 1/2),
\end{cases}
\]

In Eqs. (6) and (7), when \( k = 0 \), the common key \( c_0 \) is used.

(III) Two chaotic series are generated by the Bernoulli shift map:

\[
\begin{align*}
    x_{t+1} &= 2x_t \mod 1, \\
    y_{t+1} &= 2y_t \mod 1,
\end{align*}
\]

(8)

where \( x_0 \) and \( y_0 \) are used as the initial values. After iterating Eq. (8) \( n \) times, the \( (k+1) \)th element symbol \( c_{k+1} \) is calculated by

\[
\begin{align*}
    \text{Re}[c_{k+1}] &= x_n + b_{(k+L/2) \mod L}, \\
    \text{Im}[c_{k+1}] &= y_n + b_{((k+1)+L/2) \mod L},
\end{align*}
\]

(9)

where \( n \) is set to 100, as described in [6].
In this section, we discuss the case where the squared error is smaller than 10. The series generated by Eq. (8) converges to zero with a finite number of iterations [9]. To avoid this zero convergence, the modulo operator (mod 1) in Eq. (8) is replaced by mod(1 − 10−11), similar to [10].

In the receiver, the joint maximum likelihood sequence estimation (JMLSE) [5] is performed to decode \( \mathbf{S}_B \). The decoded block \( \mathbf{b} \) is given by

\[
\mathbf{b} = \arg \min_{\mathbf{b} \in \Omega} \sum_{i=0}^{B-1} ||r(t) - \mathbf{H}(t)\tilde{\mathbf{s}}(\mathbf{b}, c_0)||^2,
\]

where \( \Omega \) is a set of all possible bit sequences of length \( L \) and \( \tilde{\mathbf{s}}(\mathbf{b}, c_0) \) is a MIMO transmit vector generated from the block \( \mathbf{b} \) and common key \( c_0 \) in the receiver side by the chaos-based modulation described in the above-mentioned steps (I)–(V). The set of possible bit sequences \( \Omega \) and the vectors \( \tilde{\mathbf{s}}(\mathbf{b}, c_0) \) (\( \mathbf{b} \in \Omega \)) are generated in the receiver in advance.

In numerical simulations, when the double-precision floating-point number is adopted, the chaotic series generated by Eq. (8) converges to zero with a finite number of iterations [9]. To avoid this zero convergence, the modulo operator (mod 1) in Eq. (8) is replaced by mod(1 − 10−11), similar to [10].

In the original C-MIMO system, even if an eavesdropper estimates a key close to the common key \( c_0 \), the communication is still secure except when the eavesdropper estimates the common key whose squared error is smaller than 10−26 [8]. The value 10−26 is significantly small; therefore, the security is considered to be sufficient.

3. Issues in the original C-MIMO system

In this section, we discuss the case where \( N_t = 2 \), namely \( L = 2B \), for the sake of simplicity, but the same discussion is valid for the case where \( N_t > 2 \).

The following two issues exist in the original C-MIMO system:

I. Equations (6) and (7) have no effect when \( 0 < \text{Re}[c_k] < 0.5 \) and \( 0 < \text{Im}[c_k] < 0.5 \).

II. Although \( \mathbf{b} \) is composed of \( L \) bits, \( s_{k+1} \) is generated consisting of only four bits of the total \( L \) bits, namely \( b_k, b_{k+1}, b_{k+B}, \) and \( b_{k+B+1} \). This use of a small number of bits in \( \mathbf{b} \) reduces possible values of \( s_{k+1} \), which might lead to poor performance.

To resolve issue I, in Fig. 3, we show the flow for generating the transmitted symbol \( s_{k+1} \) from the element symbol \( c_k \). We first present an analysis of Eqs. (6) and (8).

First, the initial values of the chaotic dynamical systems \( x_0 \) are generated from the element symbol \( c_k \) according to Eq. (6), depending on the value of \( b_k \). After generating \( x_0 \), \( x_0 \) is mapped to \( x_1 \) by the
Bernoulli shift map (Eq. (8)). If the bit \( b_k \) affects \( s_{k+1} \), the value of \( x_1 \) must vary when the value of bit \( b_k \) varies.

However, regardless of whether \( b_k = 0 \) or \( b_k = 1 \), the values of \( x_1 \) are the same when \( 0 < \text{Re}[c_k] < 0.5 \). The following reason causes the values of \( x_1 \) to remain the same: if \( b_k = 0 \), the value of \( x_1 \) is \( 2 \times \text{Re}[c_k] \mod 1 \). Conversely, if \( b_k = 1 \), the value of \( x_1 \) is \( \{2 \times \text{Re}[c_k] + 1\} \mod 1 = 2 \times \text{Re}[c_k] \mod 1 \), which is identical to the value when \( b_k = 0 \). This is because the modulo operation is defined by \( \alpha \mod \beta \equiv \alpha - \beta \lfloor \alpha/\beta \rfloor \), where \( \lfloor \cdot \rfloor \) is the floor function. This indicates that Eq. (6) has no effect on \( s_{k+1} \) when \( 0 < \text{Re}[c_k] < 0.5 \).

To confirm the above discussion that Eq. (6) has no effect on \( s_{k+1} \) when \( 0 < \text{Re}[c_k] < 0.5 \), we plotted the value of \( x_1 \) as a function of \( \text{Re}[c_k] \) in Fig. 4. From Fig. 4, it can be observed that although the value of \( b_k \) is different, these two relations are equivalent when \( 0 < \text{Re}[c_k] < 0.5 \). Thus, regardless of whether \( b_k = 0 \) or \( b_k = 1 \), the values of \( x_1 \) are the same when \( 0 < \text{Re}[c_k] < 0.5 \).

It should be noted that the shapes of these two return maps are not important (Fig. 4(a) indicates a Bernoulli shift map and Fig. 4(b) demonstrates a tent map). The same discussion also applies to Eq. (7) when \( 0 < \text{Im}[c_k] < 0.5 \).

For issue II, we first show the constellation diagrams of the original C-MIMO system when the MIMO transmit block length \( B = 4 \) and the number of transmit and receive antennas \( N_t = N_r = 2 \). In Fig. 5, we generated and plotted \( 2^L = 2^8 \) symbols \( (s_{k+1}) \), which are all possible bit patterns of the transmit block \( b \). Even though the maximum number of symbols is \( 2^8 \), the number of symbols in Fig. 5(a) is only 16, because certain symbols take exactly the same value. Thus, it is difficult to distinguish one symbol from another. The same discussion applies to Fig. 5(b).

When generating the symbol \( s_k \), the original C-MIMO system [4–6] uses the element symbol \( c_k \) and the following four bits in \( b \): \( b_k \) in Eq. (6), \( b_{(k+1)} \mod L \) in Eq. (7), \( b_{(k+B)} \mod L \) and \( b_{((k+1)+B)} \mod L \) in Eq. (9). When \( k = 0 \), although the number of possible bit patterns of \( b \) is \( 2^L \) (\( = 2^8 \) in Fig. 5(a)),
the number of patterns of symbols $s_1$ is $2^4(=16)$. When $k=1$, the bits in $b$ used to generate the symbols $s_2$ are shifted from the bits that were used to generate the symbols $s_1$ by one bit. Hence, in addition to the four bits used in the case that $k=0$, $b_{(k+2)} \mod L$ and $b_{((k+2)+B) \mod L}$ are used to generate the symbol $s_2$. Therefore, six bits are involved in total. In Fig. 5(b), it can be observed that the number of patterns of the symbols $s_2$ is $2^6(=64)$; however, the maximum number of bit patterns of $b$ is $2^8(=256)$.

![Fig. 5. Examples of constellation diagrams for the $k$th transmitted symbol $s_k$ obtained using the original C-MIMO system, when $B=4$ and $n=100$.](image)

4. Proposed system

We propose an improved C-MIMO system that addresses the above-mentioned issues I and II discussed in Sec. 3. Figure 6 shows a configuration of the proposed chaos-based modulation for the C-MIMO transmission system.

Let us first address issue I where the third equations in Eqs. (6) and (7) have no effect on the value of $c_k$ as shown in Sec. 3. On the basis of this fact, we simply use the following Eqs. (15) and (16) instead of Eqs. (6) and (7).

\[
x_0 = \text{Re}[c_k],
\]
\[
y_0 = \text{Im}[c_k].
\]

Although issue I exists in Eqs. (6) and (7) in the original C-MIMO system from a theoretical perspective, this issue seems to be resolved indirectly by replacing the modulo operator (mod 1) in Eq. (8) with mod$(1-\delta)$ in the original C-MIMO system, where $\delta(<1)$ is a small real number and $\delta = 10^{-11}$ in [10]. This replacement of the modulo operator is introduced to prevent the values of
and $y_n$ from converging to zero in numerical simulations, but not to address issue I. Moreover, this value of $\delta$ is empirically determined; further, no reports systematically clarify how the value of $\delta$ affects the dynamics of the Bernoulli shift map and the randomness of generated transmitted symbols. In this sense, the proposed method (Eqs. (15) and (16)) can remove the uncertainty caused by the replacement of the modulo operator and simplify the original C-MIMO system.

By this change, the initial values, $x_0$ and $y_0$, are generated only from $c_k$, and the initial values do not depend on $b$ anymore. Instead, $b$ is used in another part, which resolves issue II.

Second, let us address issue II. We changed Eq. (9) to

$$c_{k+1} = x_n + i x + j y_n + i y,$$

(17)

where $n = 100$ and we adaptively change the number of iterations $i_x$ and $i_y$, using the transmit block $b$. When the $(k+1)$th element symbol $c_{k+1}$ is generated, the values of $i_x$ and $i_y$ are determined by

$$i_x = \begin{cases} 0 & (k \geq 1), \\ B - 1 \sum_{m=0}^{B-1} 2^m b_m & (k = 0), \end{cases}$$

(18)

and

$$i_y = \begin{cases} 0 & (k \geq 1), \\ 2B - 1 \sum_{m=B}^{2B-1} 2^m b_m & (k = 0). \end{cases}$$

(19)

Equations (18) and (19) indicate that $i_x$ and $i_y$ take values calculated by the second equations in Eqs. (18) and (19) only when the first transmitted symbol $s_1$ is generated ($k = 0$). We emphasize that all bits in $b$ are used in the proposed C-MIMO system. In addition, because the other transmitted symbols $s_k (k \geq 1)$ are generated from the first element symbol $c_1$, it is not necessary to calculate $i_x$ and $i_y$ for these transmitted symbols. Based on this idea, $i_x$ and $i_y$ are set to 0 when $k \geq 1$. These changes increase the number of patterns of symbols to $2^{N_t B}$, which is the maximum number of bit patterns of $b$.

5. Numerical experiments

To confirm the performance of the proposed C-MIMO system, we conducted three numerical experiments. In the first experiment, we checked the number of transmitted symbols generated from all bit patterns of $b$. Figure 7 shows the constellation diagrams obtained by the proposed C-MIMO system when the MIMO transmit block length $B = 4$.

In Fig. 7, we conducted the same experiments corresponding to Fig. 5, but used the proposed C-MIMO system instead of the original one. From Fig. 7(a) and 7(b), we can observe that the number of symbols increases substantially in comparison with Fig. 5(a) and 5(b).

Figure 8 shows distributions of inter-symbol distances obtained from the original and proposed C-MIMO systems. In the case of the original C-MIMO system, because the number of generated patterns of the symbol $s_1$ is small, the inter-symbol distances are localized around zero (Fig. 8(a)). Conversely, in the case of the proposed C-MIMO system, because the number of generated patterns of the symbol $s_1$ is $2^8$, the inter-symbol distances are widely distributed (Fig. 8(a)). From Fig. 8(b), we can observe that the tendency is almost the same. Specifically, the variation of the inter-symbol distance becomes small in the case of the original C-MIMO system. Therefore, the proposed C-MIMO system works well in increasing the number of patterns of the transmitted symbols.

In the second experiment, to show quantitatively that the proposed C-MIMO system can generate a wide variety of patterns of the transmitted symbols, we conducted the following experiment: we first calculated the transmitted symbol $s_i (i = 1, \cdots, 8)$ from $b$ using the proposed C-MIMO system. The transmitted symbols were calculated for all possible bit sequences of $b$, where the total number of patterns of $b$ is $2^{N_t B} (= 2^{8})$. Consequently, the number of patterns of each transmit symbol ($s_i$) is at most 256 patterns. Next, 256 symbols were generated randomly, where the real and imaginary parts
of each symbol obey a Gaussian distribution having the same average and variance as the symbols generated by the proposed C-MIMO system. We then calculated the distance between the distribution of inter-symbol distances obtained by the proposed C-MIMO system and that of random symbols as follows:

\[ A_i = \int_0^\infty |P_i(z) - Q(z)| \, dz, \]  

(20)

where \( P_i(z) \) is a cumulative distribution of the distances between symbols corresponding to \( s_i \) generated by the proposed C-MIMO system and \( Q(z) \) is a cumulative distribution of distances between random symbols. Because the probability that the randomly generated symbols are identical is extremely low, the 256 randomly generated symbols are predominantly different from each other. In this sense, the randomly generated symbols can be ideally placed transmitted symbols and thus the distance \( A_i \) can be a good indicator of the variation in the patterns of symbols obtained by the proposed C-MIMO system. In this experiment, by calculating Eq. (20) for the original chaos-based modulation method described in Sec. 2, we compared the proposed C-MIMO system with the original one. Figure 9 shows the averaged values of \( A_i \) calculated for 100 values of the common key \( c_0 \). From Fig. 9, it can be observed that the proposed C-MIMO system can generate symbols that are more similar to the random symbols than the symbols generated by the original C-MIMO system.

In the third experiment, we evaluated the BER and BLER of the original and proposed C-MIMO systems. In this experiment, we also investigated the BER and BLER of two MIMO systems: the first system is a MIMO system with binary phase-shift keying (BPSK) modulation and the second system is that with quadrature phase-shift keying (QPSK) modulation. We compared the proposed C-MIMO system with these two modulation schemes. In this paper, we call the MIMO system with BPSK modulation \( \text{BPSK-MIMO} \) and that with QPSK modulation \( \text{QPSK-MIMO} \). In the BPSK- and QPSK-MIMO systems, MIMO receive vectors were decoded by the maximum likelihood detection (MLD). Table I lists the simulation conditions. We assumed that the channel information follows the antenna and symbol i.i.d. one-path Rayleigh fading. In addition, the channel information is perfectly estimated in the receiver side.

Figures 10–12 show the BER and BLER against \( E_b/N_0 \) per receive antenna, where \( E_b/N_0 \) is the signal to noise ratio (SNR) per bit. In this experiment, we randomly generated \( 10^6 \) transmit blocks \( b \) and calculated their decoded blocks \( \hat{b} \). The BER is the ratio of the number of incorrect bits to the total number of received bits. Conversely, the BLER is the rate at which \( \hat{b} \) is not decoded to \( b \).
Fig. 8. Examples of distributions of inter-symbol distances when $B = 4$ and $n = 100$. The distributions illustrated in the insets in each figure are separately plotted distributions for the proposed and original C-MIMO systems.
We changed the common key $c_0$ every $10^4$ blocks (the total number of common keys $c_0$ is 100). The real and imaginary parts of the common key $c_0$ obey a uniform distribution in the range $(0, 1)$. The elements of $\mathbf{n}(t)$ are additive white Gaussian noises. Then, SNR is calculated as follows:

$$\text{SNR} = 10 \log_{10} \frac{\sigma_r^2}{\sigma_n^2}, \quad (21)$$

where $\sigma_r^2$ is the average power per receive antenna and $\sigma_n^2$ is the average power of noises. In the BPSK-MIMO, the original C-MIMO, and the proposed C-MIMO systems, $E_b/N_0$ is identical to SNR. In the case of the QPSK-MIMO system, $E_b/N_0 = \text{SNR}/2$.

We first compared the proposed C-MIMO system with the BPSK- and QPSK-MIMO systems, as illustrated in Fig. 10. From Fig. 10, it can be observed that the BPSK- and QPSK-MIMO systems exhibit better performance than the proposed C-MIMO system only when the value of SNR ($E_b/N_0$) is low ($E_b/N_0 \ll 10$). In contrast, especially in the region where the values of $E_b/N_0$ are high, the proposed C-MIMO system ($B > 2$) substantially decreases BER/BLER and shows better BER/BLER performance.
Fig. 10. Bit error rate (BER) and block error rate (BLER) of the BPSK-, the QPSK-, and the proposed C-MIMO systems, where $N_t = N_r = 2$.

Next, we compared the proposed and the original C-MIMO systems, as illustrated in Figs. 11(a) and 12(a). From Figs. 11(a) and 12(a), it can be observed that when $B = 3$ and 4, the BER and BLER performances of the proposed system are improved when compared to the original C-MIMO system. From Figs. 11(b) and 12(b), when $N_t = N_r = 3$ and 4, the BER and BLER performances of the proposed C-MIMO system are also improved when compared to the original C-MIMO system. The reason is that it is easy to distinguish transmitted symbols from each other because the number of patterns of the transmitted symbols has increased. When $B = 2$ and $N_t = 2$, the BER and BLER performances of the proposed C-MIMO system are equivalent to those of the original C-MIMO systems.

performance than the BPSK- and QPSK-MIMO systems.

Fig. 11. Comparison of the BER and BLER performances of the proposed and the original C-MIMO systems with $B = 2$, $B = 3$, and $B = 4$. (a) BER. (b) BLER.
system. This is because both the proposed C-MIMO system and the original one generate the same number of block patterns, i.e., $2^4$ block patterns, in the case where $B = 2$.

Although these results of numerical simulations reveal that the proposed C-MIMO system exhibits higher performance than the BPSK-, the QPSK-, and the original C-MIMO systems, we should specify that the computational cost of the proposed C-MIMO system is higher than that of the BPSK- and the QPSK-MIMO systems because of the high computational cost of the chaos modulation and the decoding of the modulated symbols. In addition, the computational cost of the proposed C-MIMO system is also higher than the original C-MIMO system, because the number of iterations ($i_x$ and $i_y$) is large. Consequently, reducing the computational cost of the proposed C-MIMO system is one of
In this paper, we primarily considered the single-user MIMO; however, the multi-user MIMO (MU-MIMO) [11] and massive MIMO [12–14] are currently receiving considerable attention. Besides, several extended C-MIMO systems have been proposed, where the original C-MIMO system is extended to the MU-MIMO [15] and massive MIMO systems [16]. These extended C-MIMO systems also incorporate the chaos-based modulation which is almost identical to the chaos-based modulation used in the original C-MIMO system for a single user described in Sec. 2. This fact implies that our approach can be applied to these extended C-MIMO systems. Thus, the application of our method to these extended C-MIMO systems and the evaluation of their performance are important future works.
6. Summary

In this paper, we investigated the modulation part of the C-MIMO system [4–6] from the perspective of nonlinear dynamical systems. Then, we described the issues pertaining to the initial values of the chaotic dynamical systems used in the original C-MIMO system, i.e., the constellation diagrams of the original C-MIMO system show that the same transmitted symbols are generated from different symbols because only four bits of the total \( L \) bits in the transmit block were used to generate the transmitted symbols in the original C-MIMO system.

Based on these results, we proposed a new modulation method. In the proposed C-MIMO system, all bits in the transmit block are used to generate the transmitted symbols and the number of iterations of chaotic maps was adaptively controlled by the information of the transmit block. We showed that the BER performance of the proposed C-MIMO system was superior to that of the original C-MIMO system.

Although we only evaluated the BER (BLER) performance of the proposed C-MIMO system in this paper, throughput is also an important performance measure for the proposed C-MIMO system, which should be investigated in future work.

Acknowledgments

The authors would like to thank Prof. M. Hasegawa (Tokyo University of Science) for his valuable comments and suggestions. This research is partially supported by the JSPS Grant-in-Aid for Scientific Research (Nos. 15KT0112, 17K00348 and 18K18125).

References

[1] G.J. Foschini, “Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas,” Bell Labs Technical Journal, vol. 1, no. 2, pp. 41–59, 1996.
[2] T.L. Carroll and L.M. Pecora, “Synchronizing chaotic circuits,” IEEE Transactions on Circuits and Systems, vol. 38, no. 4, pp. 453–456, 1991.
[3] G. Mazzini, G. Setti, and R. Rovatti, “Chaotic complex spreading sequences for asynchronous DS-CDMA. I. System modeling and results,” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, no. 10, pp. 937–947, 1997.
[4] E. Okamoto, “A chaos MIMO transmission scheme for channel coding and physical-layer security,” IEICE Transactions on Communications, vol. E95-B, no. 4, pp. 1384–1392, 2012.
[5] E. Okamoto and Y. Inaba, “Multilevel modulated chaos MIMO transmission scheme with physical layer security,” NOLTA, vol. 5, no. 2, pp. 140–156, 2014.
[6] E. Okamoto and N. Horiike, “Performance improvement of chaos MIMO scheme using advanced stochastic characteristics,” IEICE Communications Express, vol. 5, no. 10, pp. 371–377, 2016.
[7] G.E.P. Box and M.E. Muller, “A note on the generation of random normal deviates,” The Annals of Mathematical Statistics, vol. 29, pp. 610–611, 1958.
[8] E. Okamoto, “Performance improvement of wireless communications system using nonlinear signal processing,” IEICE Fundamental Review, vol. 9, no. 4, pp. 350–363, 2016, In Japanese.
[9] G. Alvarez and S. Li, “Breaking an encryption scheme based on chaotic baker map,” Physics Letters A, vol. 352, nos. 1–2, pp. 78–82, 2006.
[10] Y. Masuda, E. Okamoto, K. Ito, and T. Yamamoto, “An uplink non-orthogonal multiple access scheme having physical layer security based on chaos modulation,” Proceedings of 2019 International Conference on Information Networking (ICOIN), pp. 136–140, 2019.
[11] Q.H. Spencer, C.B. Peel, A.L. Swindlehurst, and M. Haardt, “An introduction to the multi-user MIMO downlink,” IEEE Communications Magazine, vol. 42, no. 10, pp. 60–67, 2004.
[12] F. Rusek et al., “Scaling up MIMO: opportunities and challenges with very large arrays,” IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 40–60, 2013.
[13] A.L. Swindlehurst, E. Ayanoglu, P. Heydari, and F. Capolino, “Millimeter-wave massive MIMO: the next wireless revolution?,” IEEE Communications Magazine, vol. 52, no. 9, pp. 56–62, 2014.
[14] E.G. Larsson, O. Edfors, F. Tufvesson, and T.L. Marzetta, “Massive MIMO for next generation wireless systems,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, 2014.

[15] Y. Inaba and E. Okamoto, “Multi-user chaos MIMO-OFDM scheme for physical layer multi-access security,” *NOLTA*, vol. 5, no. 2, pp. 172–183, 2014.

[16] N. Horiike, E. Okamoto, and T. Yamamoto, “Uplink large-scale chaos MIMO transmission scheme using gaussian belief propagation,” *Journal of Signal Processing*, vol. 22, no. 4, pp. 169–173, 2018.