

A chaos MIMO transmission scheme for secure communications on physical layer

Eiji Okamoto

Graduate School of Engineering, Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan. okamoto@nitech.ac.jp

Abstract— A secure communication is achieved by upper layer applications such as common key or public key cryptosystem in the current transmission systems. However, the security is never exclusive and the multiplexing of security schemes is highly effective, so the secure transmission scheme on physical layer is also important. One of the typical physical-layer schemes is a chaos transmission which produces a secure, safe, wired or wireless communication. However, the main drawback of the chaos scheme is the error-rate performance degradation. We proposed a chaotic convolutional code which improved the performance in the tradeoff with decoding complexity increase. Here, in this paper, we focus on the diversity property of multiple-input multiple output (MIMO) and propose a chaos MIMO transmission scheme to achieve the secure on physical layer, low error-rate, and low complexity transmission. The joint MIMO detection and chaos decoding is done by maximum likelihood decoding (MLD) at the receiver. We will evaluate the performance of proposed scheme by computer simulations.

Index Terms— chaos coded modulation, physical layer security, MIMO, maximum likelihood decoding

I. INTRODUCTION

In wireless communications, demands for high-capacity transmission are growing and various new technologies have been developed. One of those technologies is a multi-hop transmission, in which lots of terminals, such as mobile phones, forward data from the source terminal to the destination terminal. This improves the power efficiency because the distance of each wireless link becomes shorter. However, the number of the wireless links also increases and the role of wireless security, i.e., the data can be decoded only by a target user, becomes more important. Ensuring this security is never exclusive at each transmission layer and multiple uses of the secure protocol enhance the security. However, in the current systems, ensuring the security is achieved on upper layer such as XOR-scrambling generated by a common key. As the physical layer security, a spread spectrum technique [1] has been established but nowadays it is used as code division multiple access (CDMA) scheme and not used as a secure scheme.

Meanwhile, a chaos communication [2] is a well-known scheme ensuring the physical layer security. By adding the chaos signal to data signal or by modulating chaos signal by the data, the transmission signal becomes noise-wise and the secure data transmission is achieved [3]. Although it is known that the security of chaos is not complete, it can be increased by using multiple independent chaos signals [4]. Combining the

chaos scheme with upper layer secure protocols is a type of this multiple use and hence the chaos communication is an effective scheme to ensure the physical layer security. In conventional studies, the chaos schemes focusing on increasing the security have been proposed in [5] and [6]. These schemes achieve a physical layer security but the bit error rate performance is degraded due to an extra power requirement of chaos signal. In [7] and [8], a chaotic convolutional coding was proposed to improve the error rate performance and also a chaos turbo code with parallel-concatenating two chaos convolutional codes was proposed in [9] and [10]. However, in this turbo code the number of chaos state is limited to apply maximum a posteriori (MAP) decoding [11], resulting a lower security. We also proposed a chaos coded modulation scheme in [12] enabling the physical layer security and channel coding gain without limiting the number of chaos states. The coding gain can be enhanced only by increasing decoding complexity. However, to obtain a large coding gain, the sufficient decoding complexity becomes more than 2^{10} , which is relatively large. To address this problem, a complexity reduction scheme in [13] was proposed but the long error event occurred and the performance was degraded.

Here, applying chaos is available in any signal processing parts on physical layer. A multiple-input multiple-output transmission scheme [14] in which multiple antennas are used in both transmitter and receiver is used in many recent wireless systems such as cellular or WLAN. In there, MIMO is being adopted as a mandatory standard technique. In MIMO multiplexing transmission, the channel capacity can be linearly increased in proportional to the number of antennas and a large capacity transmission is achieved. A receive signal on each MIMO antenna becomes Gaussian noise-wise because of the multiplexing of multi-antenna transmission. Similarly, if some precoding schemes are applied in the MIMO transmitter to raise the capacity or transmission quality, the transmission signal also becomes noise-wise. Hence, there is no signal-processing problem in making the transmit signal noise-wise by adopting chaos into MIMO systems. If the chaos convolutional code is applied to this MIMO antenna multiplexing, a transmit diversity of MIMO is obtained so that the secure and good bit error rate (BER) performance transmission on physical layer will be achieved. As the chaos MIMO scheme, only a multiple stream transmission for a higher security has been proposed in [15] and to the best of author's knowledge, there is no study of chaos MIMO for secure channel coding. Therefore, in this paper, we propose a chaos MIMO (C-MIMO) scheme for

high-quality and secure transmission on physical layer. The number of antenna in MIMO systems is usually two or four and the constraint length of chaos coding is terminated at this number. Then, the decoding complexity is restricted at the possible range but the coding gain and physical-layer security are obtained.

In the following, the advantage and disadvantage of chaos communication are briefly discussed in Section II. The system model of the proposed scheme is introduced in Section III. Numerical results are shown in Section IV and the conclusions are drawn in Section V.

II. ADVANTAGE AND DISADVANTAGE OF CHAOS COMMUNICATION

The chaos communication used in this paper is a common key encryption system. In this chaos system, the key information such as initial value of chaos, any parameters of chaos equations is shared only with the target transmitter and receiver. The chaos encryption is processed according to the key in the transmitter. Since the chaos decryption (i.e., chaos decoding) cannot be processed correctly without the common key, the security is ensured. The chaos signals can be quantized into digital signal or unquantized as analog signal. A chaos modulation utilizes this chaos encryption where the chaos signal is modulated by transmit data. The encryption and modulation is jointly conducted and the physical layer security is ensured. However, to obtain the physical layer security each transmit signal is needed to be orthogonal, i.e., the correlation of two signals corresponding to 0 and 1 on GF(2) must be zero. This means one-half Euclidean distance, equivalent to 3 dB penalty, from an inverse correlation pair (e.g., BPSK signals). Since two signals with inverse correlation are an inversion pair of one signal, they are insecure. Thus, the zero correlation is essential to keep the physical layer security. As described in [9], this degradation of Euclidean distance is the reason why the chaos communication is not widely used. Hence, the advantage of chaos communication is ensuring the physical layer security and the disadvantage is the distance degradation as the cost of encryption. To redeem this degradation, it is necessary for the chaos modulation to compose some channel coding and we proposed a convolutional chaos coded modulation [12]. The bound of coding gain on this scheme is the Shannon limit but it needs long code length and results in unpractical decoding complexity. Thus, in order to reduce the decoding complexity of chaos coded modulation and to obtain the physical layer security and coding gain, we focus on the MIMO multiplexing. When the chaos coding is applied to MIMO multiplexing, a transmit antenna diversity effect is obtained because the transmit data loaded on each antenna are correlated, and more importantly, the number of antenna in MIMO is usually between two and eight, which means the code constraint is limited at this number. This results in a practical decoding complexity. Therefore, the proposed chaos MIMO is effective in terms of channel coding and physical layer security. In the next section, the system model is introduced.

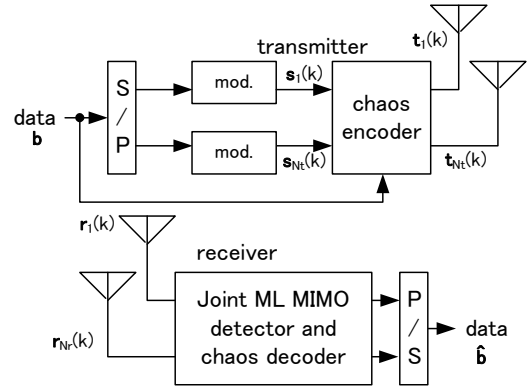


Fig. 1. C-MIMO system model.

III. SYSTEM MODEL

Fig. 1 shows the baseband system model of the proposed C-MIMO where N_t and N_r are the numbers of transmit and receive antennas, respectively. As shown in the figure, the proposed system is basically the same as conventional MIMO multiplexing system except the multiplication of chaos symbols at chaos encoder. In this scheme, a block transmission which consists of multiple MIMO vectors is used and the decoding at the receiver is done by this block unit. The number of MIMO vectors on one block is B and the bits to be transmitted on the block is

$$\mathbf{b} = [b(0) \cdots b(K-1)], \quad b(l) \in \{0,1\} \quad (1)$$

where K is the number of bits per block. If the point of modulation constellation is $A = 2^q$, K becomes $K = qB$. Here, we consider BPSK ($q=1$) and QPSK ($q=2$) cases. The data bits are serial-to-parallel transformed and loaded to each antenna. Then, the modulated symbols $s_j(k)$ are generated where k ($0 \leq k \leq B-1$) is the time and j ($1 \leq j \leq N_s$) is the antenna index. When the transmit symbol vector at time k is written by

$$\mathbf{s}(k) = [s_1(k) \cdots s_{N_s}(k)]^T \quad (2)$$

then, the transmit block matrix becomes

$$\mathbf{S} = [\mathbf{s}(0) \cdots \mathbf{s}(B-1)] \quad (3)$$

where T is a matrix transpose. The transmit block is then encrypted by a chaos matrix as follows.

$$\mathbf{T} = [\mathbf{t}(0) \cdots \mathbf{t}(B-1)] \\ = \mathbf{C} \circ \mathbf{S} \quad (4)$$

$$\mathbf{C} = \begin{bmatrix} c(1) & \cdots & c(\{B-1\}N_s + 1) \\ \vdots & \ddots & \vdots \\ c(N_s) & \cdots & c(BN_s) \end{bmatrix} \quad (5)$$

Here, \circ means scalar product (Hadamard product) of each element. and $c(k)$ is the coded chaos symbol. Finally, \mathbf{T} is transmitted. The generation of chaos matrix \mathbf{C} is described later. It is assumed that the MIMO channel is an i.i.d. quasi-static fading between every antennas and on every MIMO symbols. This time assumption will be satisfied by some additional

interleavers in practical systems. The channel matrix is given by

$$\mathbf{H}(k) = \begin{bmatrix} h_{11}(k) & \cdots & h_{1M}(k) \\ \vdots & \ddots & \vdots \\ h_{Nr1}(k) & \cdots & h_{NrM}(k) \end{bmatrix} \quad (6)$$

and the receive block $(N_r \times B)$ -matrix is composed by

$$\mathbf{R} = [\mathbf{r}(0) \cdots \mathbf{r}(B-1)]$$

$$\mathbf{r}(k) = [r_1(k) \cdots r_{N_r}(k)]^T \quad (7)$$

where $r_i(k)$ is i -th antenna receive symbol. The noise block is similarly given by

$$\mathbf{N}(k) = [\mathbf{n}(0) \cdots \mathbf{n}(B-1)]$$

$$\mathbf{n}(k) = [n_1(k) \cdots n_{N_r}(k)]^T \quad (8)$$

where each $n_i(k)$ is i.i.d. additive white Gaussian noise (AWGN). Then, the receive vector can be written by

$$\mathbf{r}(k) = \mathbf{H}(k)\mathbf{t}(k) + \mathbf{n}(k) \quad (9)$$

In the receiver, the joint maximum likelihood (ML) MIMO detection and chaos decoding is conducted by

$$\hat{\mathbf{b}} = \arg \min_b \|\mathbf{R} - \mathbf{H}\mathbf{T}\|_F^2 \quad (10)$$

$$\mathbf{H} = [\mathbf{H}(0) \cdots \mathbf{H}(B-1)]$$

$$\mathbf{T} = \begin{bmatrix} \mathbf{t}(0) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{t}(1) & & \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \cdots & & \mathbf{t}(B-1) \end{bmatrix}$$

where $\|\cdot\|_F$ is the Frobenius norm and from (1), the number of decoding search becomes 2^K .

The generation of chaos symbols is based on Bernoulli shift map [7,8]. Each symbol of \mathbf{C} is made as a unit vector by

$$c(k) = \exp\{j2\pi \tan^{-1}(\text{Im}[s_k]/\text{Re}[s_k])\} \quad (11)$$

$$s_k = \frac{1}{M} \sum_{i=0}^{M-1} \{(\text{Re}[c_{ki}] + \text{Im}[c_{ki}]) \exp(j2\pi[\text{Re}[c_{ki}] - \text{Im}[c_{ki}]])\} \quad (12)$$

where k is $1 \leq k \leq BN_s$ and c_{ki} is an M -element chaos symbol used to generate a Gaussian noise vector s_k . M is the number of independent chaos signals used for making white noise by central limit theorem, and is set to relatively large value. Since $c(k)$ is a unit vector, the encryption of \mathbf{S} is conducted by the random phase shift which doesn't change the average transmit power. Each chaos symbol c_{ki} is given by M -element chaos vector as

$$\mathbf{c}_M(k) = [c_{k0} \cdots c_{k(M-1)}], \quad c_{ki} \in \mathbb{C}, \quad 0 < \text{Re}[c_{ki}], \text{Im}[c_{ki}] < 1 \quad (13)$$

and the source and destination terminals have the same initial vector

$$\mathbf{c}_M(0) = [c_{00} \cdots c_{0(M-1)}] \quad (14)$$

Thus, the proposed scheme is categorized as the common key encryption and $\mathbf{c}_M(0)$ in (14) is the key signal, which can also be quantized. Then, the chaos vector $\mathbf{c}_M(k)$ is iteratively modulated by the chaos convolution with transmit data as

$$\mathbf{c}_M(k) = f(\mathbf{c}_M(k-1), \mathbf{b}_k) \quad (15)$$

where f is the iteration function and \mathbf{b}_k is a partial cyclic shift version of data bits \mathbf{b} given by

$$\mathbf{b}_k = [b_k(1), \dots, b_k(q)]$$

$$= [b(\{k+K-q\} \bmod K), \dots, b(\{k+K-1\} \bmod K)]$$

The chaos transition of (15) is conducted independently in real and imaginary parts by Bernoulli shift map. The real part is given as follows.

$$x_0 = \begin{cases} \text{Re}[c_{(k-1)i}] & (b_k(1) = 0) \\ \text{Re}[c_{(k-1)i}] - 1/2 & (b_k(1) = 1, \text{Re}[c_{(k-1)i}] > 1/2) \\ 1 - \text{Re}[c_{(k-1)i}] & (b_k(1) = 1, \text{Re}[c_{(k-1)i}] \leq 1/2) \end{cases} \quad (16)$$

$$x_{l+1} = 2x_l \bmod 1 \quad (17)$$

$$\text{Re}[c_{ki}] = x_{18} \quad (18)$$

where (16) is the chaos modulation. The imaginary part is the same as (16)-(18); if BPSK is used, only (17) is used for the imaginary part, or if QPSK is used, the modulation of (16) with $b_k(2)$ is used. Note that (17) is the Bernoulli chaos shift transition. This configuration of chaos was determined by numerical search as the phase of $c(k)$ had a uniform distribution. This condition is easy to satisfy and the equations of (11), (12), (16), and (18) can be relatively freely changed, the error rate performance is slightly affected, though. Therefore, the configuration of this paper is one of the examples and the above settings were numerically determined to have a better error rate performance. It is also possible that these configurations themselves are treated as the common key which only the transmitter and receiver know.

Here, a linear nulling scheme of inverse matrix multiplication exists for MIMO detection other than MLD as a low complexity scheme. However, since the chaos block coding is applied as shown in (4) and (5) in the proposed scheme, the symbol-wise detection and decoding cannot be utilized and the sequential decoding of (10) is needed. To enable the symbol-wise MIMO detection and decoding, the chaos coding should be symbol-by-symbol, that is, code constraint must be 1. In this case, however, the coding gain is not sufficiently obtained and the error rate performance is degraded. Thus, the MLD is adopted here.

IV. NUMERICAL RESULTS

The performances of the proposed scheme are evaluated by computer simulations where the simulation conditions are listed in Table I. It is assumed the channel is perfectly known at the receiver and the initial chaos is synchronized between the transmitter and receiver. To obtain the average performance, the initial key vector of (14) is randomly changed at every block in this simulation. As a concatenation code outside of Fig. 1, no coding and convolutional coding (CC) with the memory length $K_c=2$ and code length $L=200$ are considered. In decoding, (10) is conducted in the uncoded case and the Euclidean distance-based Viterbi decoding where all combinations of C-MIMO-MLD are corresponding to each state of trellis diagram is conducted in the convolutional coding case. Table II

Tab. I. Simulation parameters.

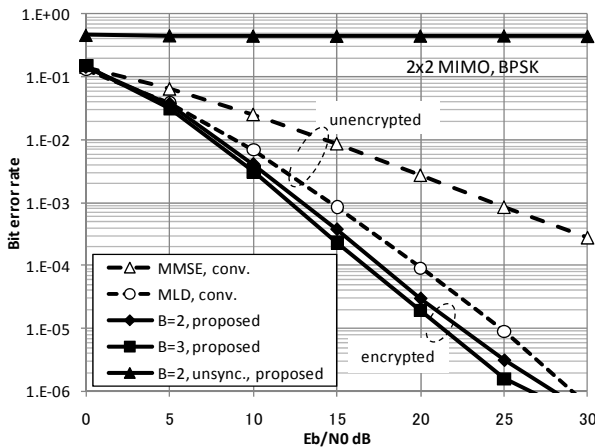
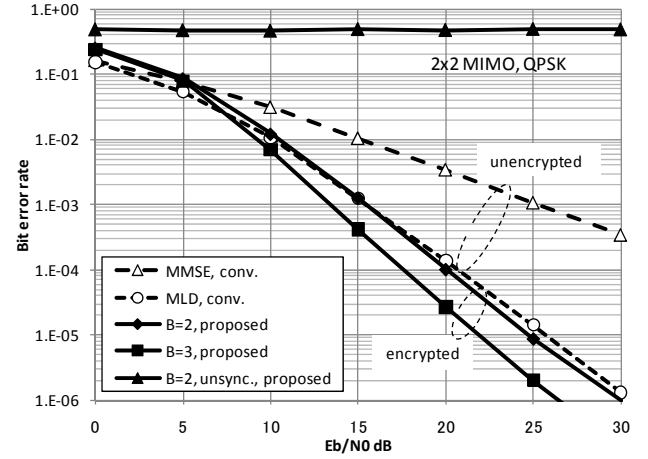
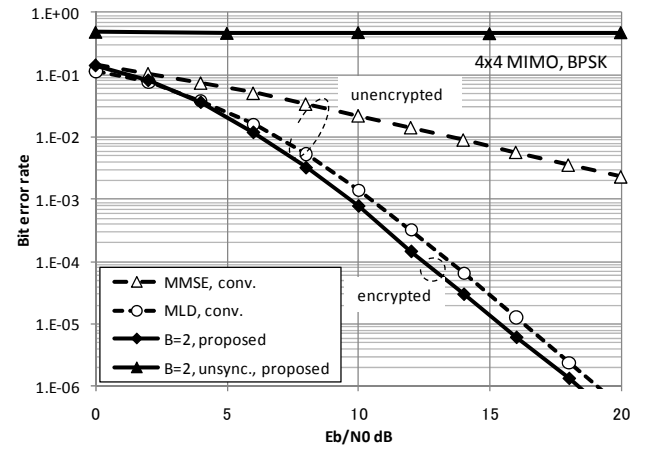
modulation	BPSK($q=1$), QPSK($q=2$)
num. of antenna	$N_t=N_r=2, 4$
num. of MIMO symbols on 1 block	$B=2, 3, 4, 5$
chaos	Bernoulli shift map
num. of chaos signals	$M=10$
initial chaos sync.	perfect
channel	i.i.d. quasi-static flat Rayleigh fading
receive channel state inf. (CSI)	perfect
channel coding	uncoded convolutional code NSC[7 5], rate=1/2, $L=200$ $K_c=2$, soft Viterbi decoding

Tab. II. Comparison of decoding complexity.

	proposed	conventional
system	C-MIMO-MLD	MIMO-MLD
uncoded	2^{qBN_t}	2^{qN_t}
NSC coded	$2^{\max(qBN_t, K_c)} L$	$2^{\max(qN_t, K_c)} L$

shows the comparison of the number of decoding search as the decoding complexity. In MIMO-MLD it is based on an exponential search of transmit bits or trellis states, while in C-MIMO-MLD it is exponentially increased due to the block decoding of B compared with MIMO-MLD. The incremental value is dependent on the modulation q and the number of transmit antenna N_t .

First, we compare the minimum squared Euclidean distances of MIMO-MLD of \mathcal{S} and C-MIMO-MLD of \mathcal{T} with $N_t = N_r = 2$, $B=1$ and BPSK as 1st modulation. The results of 10^4 block average are 4.0 and 2.8, respectively. Consequently, the average distance property is nearly a half of BPSK and it is expected that the bit error rate (BER) performance will be better than MIMO-MLD with $B=2$ and more as considered in Section II.

Fig. 2. BER performances with $N_t=N_r=2$ and BPSK.Fig. 3. BER performances with $N_t=N_r=2$ and QPSK.Fig. 4. BER performances with $N_t=N_r=4$ and BPSK.

Figs. 2 and 3 show the BER performances versus E_b/N_0 of BPSK and QPSK, respectively, with $N_t=N_r=2$ and the parameter of B . In both cases, the proposed scheme has an encryption effect and coding gain for the conventional unencrypted MIMO-MLD. The coding gains of BPSK with $B=2$ and 3 are 2.5 dB and 3.5 dB, respectively, at BER of 10^{-5} . Similarly, those of QPSK with $B=2$ and 3 are 1.1 dB and 3.1 dB. The BER of the case that M -initial key symbols are 10^{-3} different from those of transmitter is almost 0.5, which means the transmit data cannot be decoded correctly even if the difference of the key in (14) is very small and the physical layer security is ensured.

Next, Fig. 4 shows the BER of $N_t=N_r=4$ and BPSK. The performance improvement is kept as 0.8 dB gain with $B=2$ at BER of 10^{-5} . Hence, the transmit antenna diversity and coding gain are obtained by chaos coding compared with the conventional MIMO multiplexing. Since the Euclidean distance becomes half by the chaos modulation as described in Section II, the performance improvement is obtained with $B=2$, i.e., by utilizing the longer chaos code length and time diversity effect of fading. Numerical results showed that the sufficient effect was obtained with $B=2$. The proposed scheme has the physical layer security and coding gain which the conventional

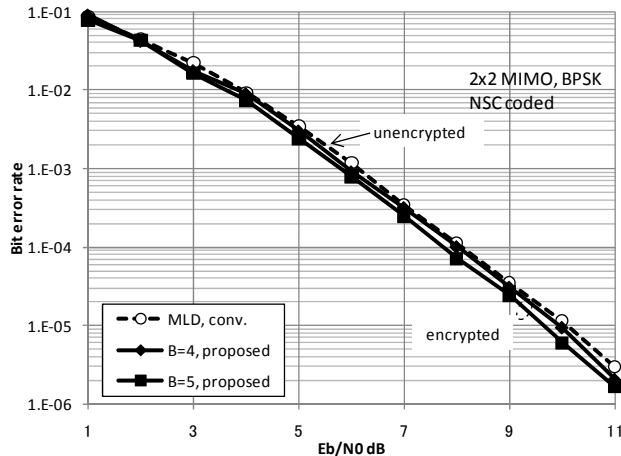


Fig. 5. BER performances with outer convolutional code.

scheme doesn't have. When the transmit antenna N_t increases, a larger gain will be obtained by the transmit antenna diversity effect and $B=2$ will be sufficient though the decoding complexity of MLD is also increased. However, as shown in Fig. 4, the coding gain is decreased compared with $N_t=N_r=2$ of Fig. 2 because the path diversity effect of maximum ratio combining (MRC) in the receiver is also increased.

Fig. 5 shows the performance comparison with outer CC. When the block length B is longer than the convolutional code constraint length, i.e., $B \geq 4$, the coding gain is obtained. The chaos coding gains are 0.12 dB and 0.46 dB at BER of 10^{-5} with $B=4$ and 5, respectively. Since the chaos coding length is longer than the CC constraint length, the minimum error event path of CC is effectively corrected by the chaos code. Thus, even in channel coding systems, the proposed scheme can obtain the performance improvement with $B > K_c + 1$. Note that if the decoding scheme of outer code is hard-decision type, this constraint length condition is released. The combined MLD is needed when the soft-decision decoding is adopted as this example. It is expected that a serial-concatenated iterative component decoding with log-likelihood ratio (LLR) can be adopted for C-MIMO.

V. CONCLUSION

In this paper, we proposed the chaos MIMO transmission scheme achieving a high-quality, large capacity, and secure communication on physical layer by adopting the chaos coding into MIMO multiplexing. The performance improvement was clarified by computer simulations. We showed that the coding gain and physical layer security was obtained in tradeoff with decoding complexity increase and the block length of $B=2$ was sufficient in this simulation. In the condition of BPSK, $B=2$, and $N_t=N_r=2$, the numbers of ML decoding search in the conventional and the proposed schemes are 4 and 16, respectively, which is 4 times of conventional scheme. This

increase is sufficiently admissible. In the proposed scheme, only chaos multiplication to each MIMO transmit symbols is needed, which is a little additional mechanism. Similarly, only the MLD with chaos is needed in the receiver. Thus, the implementation of the proposed scheme to MIMO system is straightforward.

For further studies, composing C-MIMO-OFDM for multipath fading channel and introducing LLR for iterative MIMO detection and longer code decoding such as low-density parity check (LDPC) code will be considered.

ACKNOWLEDGMENT

This research was partially supported by KDDI foundation. The author wishes to thank for their support.

REFERENCES

- [1] R. C. Dixon, "Spread Spectrum Systems," Wiley, 1976.
- [2] T. L. Carroll, L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Cir. Sys.*, vol. 38, no. 4, pp. 453-456, Apr. 1991.
- [3] R. Kharel, S. Rajbhandari, Z. Ghassemlooy, and K. Busawon, "Digitization of chaotic signal for reliable communication in non-ideal channels," *Proc. Int'l Conf. on Transparent Optical Networks, Mediterranean Winter 2008 (ICTON- MW'08)*, pp. Sa1.2 (1-6), Dec., 2008.
- [4] T. Yang, "A survey of chaotic secure communication systems," *Int. J. Comp. Cognition*, vol. 2, pp. 81-130, Jun. 2004.
- [5] H. Dedieu, M. P. Kennedy and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Cir. Sys.*, vol. 40, no. 10, pp. 634-641, Oct. 1993.
- [6] G. Kolumban and M.P. Kennedy, "Recent results for chaotic modulation schemes," *Proc. IEEE Intl. symp. on Cir. Sys.*, vol. 3, pp 141-144, May 2001.
- [7] B. Chen and G. W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," *IEEE Trans. Comm.*, Volume 46, Issue 7, July 1998 Page(s):881-890.
- [8] S. Kozic, T. Schimming, and M. Hasler, "Controlled One- and Multidimensional Modulations Using Chaotic Maps," *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, vol. 53, no. 9, pp. 2048- 2059, 2006.
- [9] F. J. Escibano, L. López, and M. A. F. Sanjuán, "Iteratively decoding chaos encoded binary signals," in *Proc. Eighth IEEE International Symposium on Signal Processing and Its Applications (ISSPA) 2005*, vol. 1, Sydney, Australia, pp. 275-278, Aug. 2005.
- [10] F. J. Escibano, S. Kozic, L. López, M. A. F. Sanjuán, M. Hasler, "Turbo-like structures for chaos encoding and decoding," *IEEE Trans. on Communications*, vol. 57 no. 3, p.597-601, Mar. 2009.
- [11] F. J. Escibano, L. López, and M. A. F. Sanjuán, "Exploiting symbolic dynamics in chaos coded communications with maximum a posteriori algorithm," *Electron. Lett.*, Vol. 42, Issue 17, pp. 984-986, Aug. 2006.
- [12] E. Okamoto and Y. Iwanami, "A trellis-coded chaotic modulation scheme," *Proc. IEEE Int'l Conf. Commun.*, vol.11, pp.5010-5015, Jun. 2006.
- [13] E. Okamoto and Y. Iwanami, "Study on MAP decoding for component code on chaotic coded modulation," *Technical Report of IEICE*, vol. 108, no. 336, NLP2008-84, pp. 75-80, Dec. 2008 (In Japanese).
- [14] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multiple antennas," *Bell Labs Syst. Tech. J.*, vol. 1, pp. 41-59, 1996.
- [15] G. Zheng, D. Boutat, T. Floquet, J.-P. Barbot, *Secure Communication Based on Multi-input Multi-output. Chaotic System with Large Message Amplitude*, *Chaos, Solitons & Fractals*, Vol. 41, No 3, pp. 1510-1517, 2009.