An M-ary Transmission Scheme for Chaotic Communications

Kai Y. Cheong, Francis C.M. Lau and Chi K. Tse *

Abstract — **This paper proposes an M-ary chaotic-sequence spread-spectrum modulation scheme. In this scheme, each block of chaotic sequence produced by a chaotic map undergoes a transformation before it is transmitted. Information is carried by the choice of transformation used. Both coherent and noncoherent implementations are considered. The performances of the systems are studied by computer simulations.**

1 INTRODUCTION

Over the last decade, extensive research has been conducted on the application of chaos in spread-spectrum communication systems [1, 2]. A direct application of chaos to the existing direct-sequence spread-spectrum system is to replace the binary sequences for spreading binary symbols by aperiodic chaotic sequences [3]. To improve the bandwidth efficiency of such a chaotic-sequence spread-spectrum (CSSS) system, transmitting M-ary symbols may be prefered over binary ones. One approach is to install M chaos generators at the transmitter to generate sequences representing the M symbols. If these chaotic sequences can be reproduced at the receiver, a correlator-type demodulator can be employed to decode the received signal [4]. Otherwise, some noncoherent detection techniques have to be used [5]. The main drawback of the aforementioned M-ary system is that the number of chaos generators increases with the symbol number M, which in turn increases the complexity of the modulator and demodulator.

In this paper, we propose an M-ary transmission scheme which employs only one chaos generator. Each block of chaotic sequence will undergo a transformation process before it is transmitted. The transformation used for each symbol is different, thus allowing the symbol to be distinguished in the receiver which uses the appropriate inverse transformation for decoding that symbol. In our proposal, a set of permutation-based transformations are used. Both coherent and noncoherent types of modulation/demodulation techniques are considered in this study.

*Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hunghom, Kowloon, Hong Kong, China. Email: 01900720r@polyu.edu.hk, encmlau@polyu.edu.hk & encktse@polyu.edu.hk

2 SYSTEM DESCRIPTION

Figure 1 shows the block diagram of an M-ary chaotic-sequence spread-spectrum communication system. On the transmitting side, each sequence block produced from the chaos generator undergoes a certain reversible transformation. Each symbol corresponds to a different transformation. Based on the incoming sequence block, the receiver attempts to determine the most probable transformation that has been used in the transmitter and then decodes the symbol. A synchronization signal, shown as dashed line in the diagram, is normally required in the case of coherent detection.

2.1 Coherent System

We consider the coherent system in this section. Assume that the chaotic sequences generated at the transmitter can be reproduced exactly at the receiver. Let β be the spreading factor, defined as the number of chaotic samples sent for each M-ary symbol. Let the generator output be denoted by x_k at time k. During the lth bit duration, i.e., for time $k = \beta(l-1)+1, \beta(l-1)+2, \ldots, \beta l$, the output block from the generator, $\boldsymbol{x}_l$, is

$$\boldsymbol{x}_l = (x_{\beta(l-1)+1} \;\; x_{\beta(l-1)+2} \;\; \cdots \;\; x_{\beta l}). \qquad (1)$$

This sequence block will undergo a transformation before transmission. In our system, we propose to operate a simple permutation on the block. For example, to send the digital symbol $i \in \{1, 2, \cdots, M\}$, the sequence block undergoes a transformation F_i. The block of chaotic sequence transmitted, $\boldsymbol{u}_l$, equals

$$\begin{aligned} \boldsymbol{u}_l &= (u_{\beta(l-1)+1} \;\; u_{\beta(l-1)+2} \;\; \cdots \;\; u_{\beta l}) \\ &= F_i(\boldsymbol{x}_l) = \boldsymbol{x}_l \boldsymbol{P}_i \end{aligned} \qquad (2)$$

where $\boldsymbol{P}_i$ is a permutation matrix.[1] The construction of the permutation matrices used in our system can be found in the appendix.

Assuming an additive white Gaussian noise (AWGN) channel, the block of chaotic sequence collected by the receiver, $\boldsymbol{v}_l$, is $\boldsymbol{v}_l = \boldsymbol{u}_l + \Psi_l$. Here, Ψ_l

[1] A permutation matrix is defined as a square matrix whose elements are either "0" or "1", with each row and column containing exactly one "1" [6].

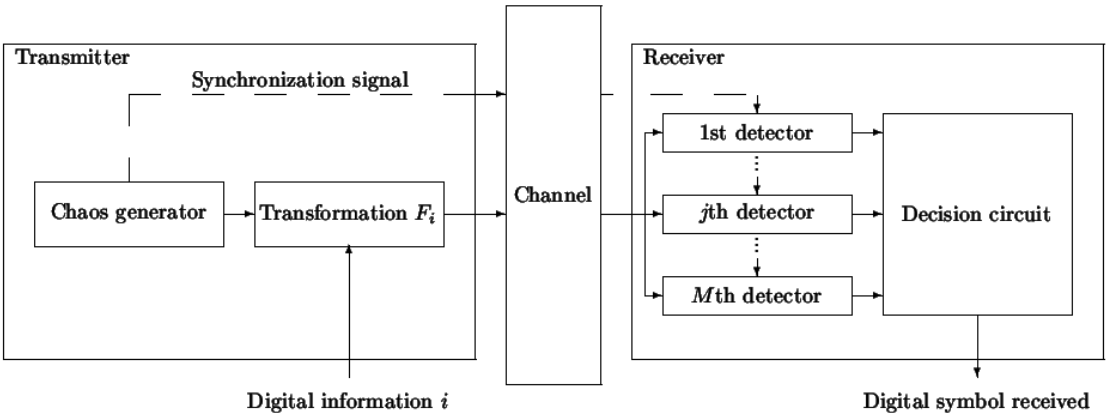

Fig. 1: Block diagram of an M-ary chaotic-sequence spread-spectrum (CSSS) communication system.

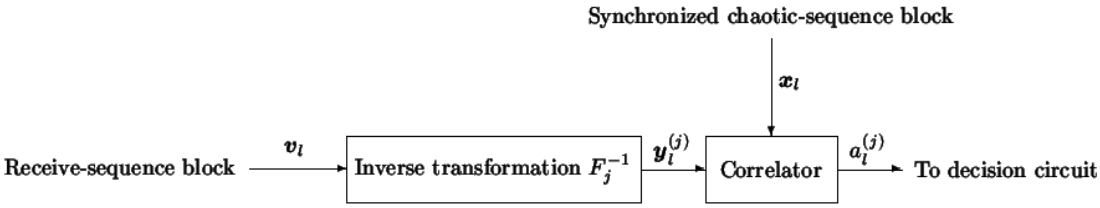

Fig. 2: Block diagram of the jth detector in the coherent M-ary CSSS system.

is defined as

$$\Psi_l = (\xi_{\beta(l-1)+1} \;\; \xi_{\beta(l-1)+2} \;\; \cdots \;\; \xi_{\beta l}) \qquad (3)$$

where ξ_k is an independent Gaussian noise sample with zero mean and variance $N_0/2$. The job of the receiver now is to determine the received symbol from the received sequence block $\boldsymbol{v}_l$. As shown in Figure 1, the received sequence block is sent to M detectors in parallel. Based on the detectors' outputs, the decision circuit determines the received symbol. Figure 2 shows the jth detector, which consists of an inverse transformation process and a correlator. The output of the inverse transformation block is

$$\boldsymbol{y}_l^{(j)} = F_j^{-1}(\boldsymbol{v}_l) = \boldsymbol{v}_l \boldsymbol{P}_j^{-1} = \boldsymbol{x}_l \boldsymbol{P}_i \boldsymbol{P}_j^T + \Psi_l \boldsymbol{P}_j^T. \quad (4)$$

Note that the inverse of a permutation matrix equals the transpose of the matrix. The second part of the detector then calculates the correlation between $\boldsymbol{y}_l^{(j)}$ and $\boldsymbol{x}_l$. For the lth symbol, the output of the jth detector, $a_l^{(j)}$, is given by

$$a_l^{(j)} = \boldsymbol{y}_l^{(j)} \boldsymbol{x}_l^T = \boldsymbol{x}_l \boldsymbol{P}_i \boldsymbol{P}_j^T \boldsymbol{x}_l^T + \Psi_l \boldsymbol{P}_j^T \boldsymbol{x}_l^T. \qquad (5)$$

From (5), we see that the correlation between $\boldsymbol{y}_l^{(j)}$ and $\boldsymbol{x}_l$ is low when $j \neq i$, and is high when $j = i$. Thus the correlator output $a_l^{(j)}$ for the case $j = i$ should be the largest and the symbol received can be decoded accordingly by the decision circuit.

2.2 Noncoherent System

Chaos synchronization is difficult to achieve when the channel has poor propagation condition. In such cases, a noncoherent modulation/demodulation scheme is preferred. The working principle of the noncoherent version of the M-ary system is similar to that used in the noncoherent differential chaos-shift-keying (DCSK) system [2], in which a reference signal and an information-bearing signal are sent consecutively during a symbol duration. In our M-ary system, the reference sequence block is chaotic, while the information-bearing block is a permutation of the reference sequence block.

For notational convenience, we denote the spreading factor by 2β in the noncoherent system. The block diagram of the noncoherent system is depicted in Figure 3. Using the same notations as in Section 2.1, during the lth symbol duration, the chaos generator generates a block of chaotic sequence, denoted by $\boldsymbol{x}_l$, which is used as the reference sequence block here. The sender then generates an information-bearing sequence block by

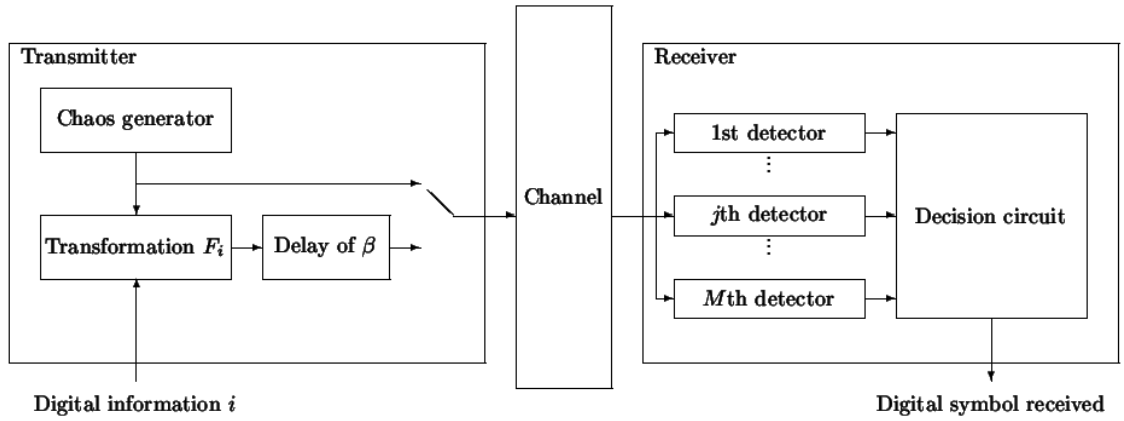

Fig. 3: Block diagram of a noncoherent M-ary CSSS system.

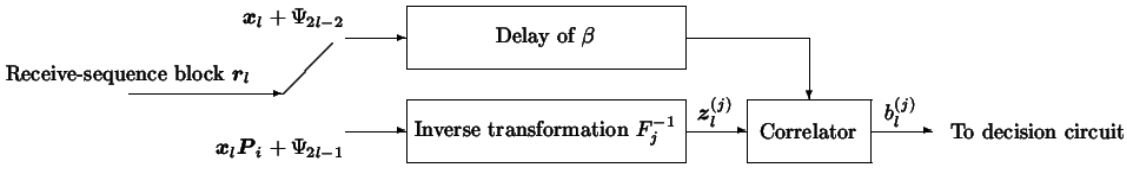

Fig. 4: Block diagram of the jth detector in a noncoherent M-ary CSSS system.

applying a transformation to the reference block according to the symbol being transmitted. Both the reference and the information-bearing sequence blocks are sent to the channel, each occupying half the symbol duration. Now suppose we are transmitting symbol i. The sequence block sent to the channel during the lth symbol duration, $\boldsymbol{s}_l$, is given by

$$\boldsymbol{s}_l = (\boldsymbol{x}_l \;\; F_i(\boldsymbol{x}_l)) = (\boldsymbol{x}_l \;\; \boldsymbol{x}_l \boldsymbol{P}_i). \tag{6}$$

The received sequence block, $\boldsymbol{r}_l$, is

$$\begin{aligned} \boldsymbol{r}_l &= \boldsymbol{s}_l + (\Psi_{2l-2} \;\; \Psi_{2l-1}) \\ &= (\boldsymbol{x}_l + \Psi_{2l-2} \;\; \boldsymbol{x}_l \boldsymbol{P}_i + \Psi_{2l-1}). \end{aligned} \tag{7}$$

In the receiver, as shown in Figure 4, the jth detector performs an inverse transformation on the received information-bearing part of the sequence block. The output block, $\boldsymbol{z}_l^{(j)}$, is given by

$$\begin{aligned} \boldsymbol{z}_l^{(j)} &= F_j^{-1}(\boldsymbol{x}_l \boldsymbol{P}_i + \Psi_{2l-1}) \\ &= \boldsymbol{x}_l \boldsymbol{P}_i \boldsymbol{P}_j^T + \Psi_{2l-1} \boldsymbol{P}_j^T. \end{aligned} \tag{8}$$

Finally, the detector output, $b_l^{(j)}$, is the correlation of $\boldsymbol{z}_l^{(j)}$ and the reference part of the sequence block, i.e.,

$$\begin{aligned} b_l^{(j)} &= \boldsymbol{z}_l^{(j)} (\boldsymbol{x}_l + \Psi_{2l-2})^T \\ &= \boldsymbol{x}_l \boldsymbol{P}_i \boldsymbol{P}_j^T \boldsymbol{x}_l^T + \boldsymbol{x}_l \boldsymbol{P}_i \boldsymbol{P}_j^T \Psi_{2l-2}^T \\ &\quad + \Psi_{2l-1} \boldsymbol{P}_j^T \boldsymbol{x}_l^T + \Psi_{2l-1} \boldsymbol{P}_j^T \Psi_{2l-2}^T. \end{aligned} \tag{9}$$

From (9), it can be concluded that the value of $b_l^{(j)}$ is small when $j \neq i$, and is large when $j = i$. The decision circuit can then identify the symbol according to $b_l^{(j)}$.

3 SIMULATION RESULTS

In this section, we study the performance of the proposed M-ary system by computer simulations. The logistic map

$$x_{k+1} = 1 - 2x_k^2 \tag{10}$$

is used to generate the chaotic sequences. For fair comparison, we keep the number of chaotic samples per bit (N) to be identical in all systems. In our simulations, we use $N = 40$. Also, the relation $\gamma = N \log_2 M$ holds, where γ represents the spreading factor of each symbol. In our case, γ is equal to β and 2β in the coherent and noncoherent system, respectively.

Denoting the average power of the chaotic samples by σ_s^2, the average bit energy (E_b) equals $N\sigma_s^2$. The system performance is shown by plotting the bit error rate (BER) against the average-bit-energy-to-noise-power-spectral-density ratio (E_b/N_0). For the M-ary systems, the symbols are converted back to bits when measuring the BER.

Figures 5 and 6 show the simulation results for the coherent and noncoherent M-ary CSSS systems, respectively. As expected, the performance

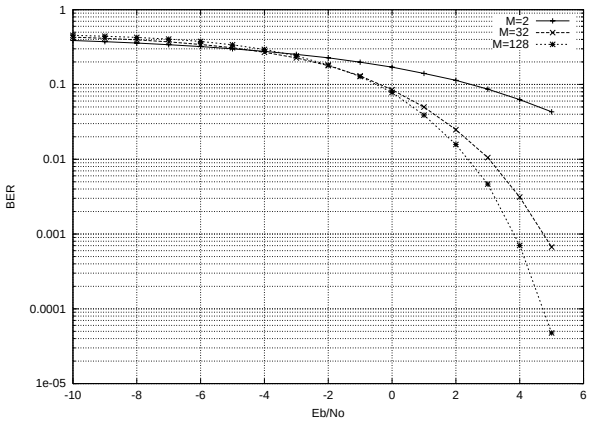

Fig. 5: Bit error rates versus E_b/N_0 of a coherent M-ary CSSS communication system.

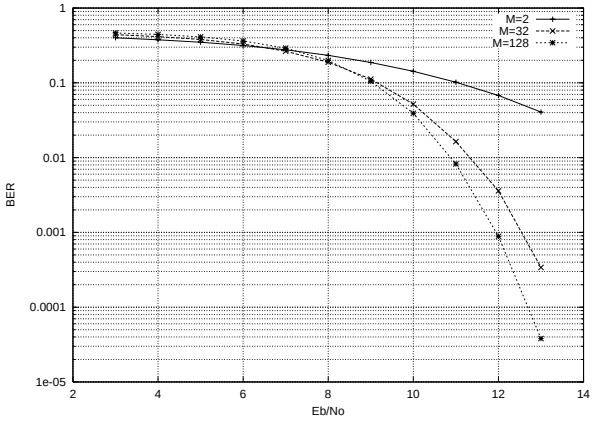

Fig. 6: Bit error rates versus E_b/N_0 of a noncoherent M-ary CSSS communication system.

of a noncoherent system is worse than that of a coherent system. Also, the performance of the M-ary system improves as M increases from 2 to 128.

4 CONCLUSION

In this paper, a permutation-based M-ary chaotic-sequence spread-spectrum communication scheme is proposed. Only one chaos generator and M linear transformations are involved in the transmitter. Both coherent and noncoherent systems have been considered. Computer simulations indicate that the bit error rate can be improved by transmitting more than one bit per symbol.

APPENDIX: CONSTRUCTION OF PERMUTATION MATRICES

This appendix defines the set of permutation matrices used in the paper. A permutation matrix is a square matrix whose elements are either "0" or 1, with exactly one "1" in each row and each column. Our objective here is to find a set of permutation matrices $\boldsymbol{P}_k$ for $k \in \{1, 2, \cdots, M\}$ such that the correlation between $\boldsymbol{x}\boldsymbol{P}_i\boldsymbol{P}_j^T$ and $\boldsymbol{x}$ is kept to a low value when $i \neq j$. This requires that the λth element in $\boldsymbol{x}\boldsymbol{P}_i\boldsymbol{P}_j^T$ is not equal to the λth element in $\boldsymbol{x}$ for all λ.

Define $\boldsymbol{R}$ as a random permutation matrix of size $N \times N$ and $\boldsymbol{A}$ as the "shifting" permutation matrix of size $N \times N$ where

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}. \qquad (11)$$

Note that the consequence of multiplying $\boldsymbol{A}$ to a vector $(x_1 \quad x_2 \quad \ldots \quad x_N)$ k times is equivalent to shifting the elements in the array to the right k times with the overflown elements being re-inserted from the left. Now, the permutation matrices are constructed using $\boldsymbol{P}_k = \boldsymbol{R}\boldsymbol{A}^k$ Also, $\boldsymbol{P}_i\boldsymbol{P}_j^T = \boldsymbol{R}\boldsymbol{A}^{i-j}\boldsymbol{R}^T$ and it can be readily shown that the diagonal elements of $\boldsymbol{R}\boldsymbol{A}^{i-j}\boldsymbol{R}^T$ are all zeros when $i \neq j$. Under such a circumstance, all elements in $\boldsymbol{x}$ will move to new positions when multiplied by $\boldsymbol{P}_i\boldsymbol{P}_j^T$ as long as $M \leq N$.

References

[1] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. of Bifurc. and Chaos,* vol. 2, pp. 709–713, 1992.

[2] G. Kolumbán, M.P. Kennedy and L.O. Chua, "The role of synchronization in digital communications using chaos — Part II: Chaotic modulation and chaotic synchronization," *IEEE Trans. Cir. and Sys. - I,* vol. 45, no. 11, pp. 1129–1140, 1998.

[3] U. Parlitz and S. Ergezinger, "Robust communication based on chaotic spreading sequences," *Phys. Lett.,* vol. A188, pp. 146–150, 1994.

[4] F.C.M Lau and C.K. Tse, "Optimum correlator-type receiver design for CSK communication systems," *Int. J. of Bifurc. and Chaos,* vol.12, no.5, pp. 1029–1038, 2002.

[5] M. Hasler and T. Schimming, "Chaos communication over noisy channels," *Int. J. of Bifurc. and Chaos,* vol. 10, pp. 719–735, 2000.

[6] G.W. Stewart, *Matrix Algorithms,* Philadelphia: Society for Industrial and Applied Mathematics, 1998.