Return-Map-Based Approaches for Noncoherent Detection in Chaotic Digital Communications

C. K. Tse, F. C. M. Lau, K. Y. Cheong, and S. F. Hau

***Abstract*—In this brief, simple noncoherent detection methods for chaos-shift-keying (CSK) modulation are proposed. By exploiting some deterministic property of the two chaotic maps, the proposed methods recover the digital message through simple decision algorithms. Specifically, the proposed methods exploit the difference in the return maps of the signals representing the digital symbols. Two specific algorithms are discussed, namely a regression-based algorithm and a probability-based algorithm. Simple tent maps are used for illustration. The bit-error-rate under additive white Gaussian noise is studied by computer simulations.**

***Index Terms*—Chaos-based communication, digital communication, error probability, least-squares regression, noncoherent detection, return maps.**

I. Introduction

In a chaos-shift-keying (CSK) communication system, M digital symbols are represented by chaotic signals generated from M dynamical systems or from one system with M different parameter values [1], [2]. In the binary case, i.e., $M = 2$, the transmitted signal essentially switches between two chaotic signals, which are generated from two dynamical systems or from one dynamical system having a parameter switched between two values, according to the digital symbol to be represented. Detection can take either a coherent form or a noncoherent form. In coherent detection, the receiver is required to reproduce the same chaotic signals sent by the transmitter, often through a "chaos synchronization" process which is unfortunately not easily implemented with sufficient robustness [3]. Once reproduced, the digital symbols can be recovered by standard correlation detection [4]–[7]. In noncoherent detection of CSK, however, the receiver does not have to reproduce the chaotic signals. Rather, it makes use of some distinguishable property of the chaotic signals to determine the identity of the digital symbol being transmitted. The most commonly exploited distinguishable property has been the bit energy [8], [9]. However, when bit energy is chosen as the distinguishable property, detection can be accomplished easily by intruders, jeopardizing the security of the system.

For a differential CSK system, it has been shown that suitable exploitation of the determinism of the chaotic signals can lead to improved performance [10]. In this brief, we consider noncoherent detection of CSK, and in particular, we make use of the *built-in determinism* of the chaotic signals for demodulation. In particular, the return map is used to distinguish the digital symbols. Specific algorithms are developed, based on simple regression and probability calculation. Illustrative examples are given using the tent maps as the chaos generator, and computer simulations are used to evaluate the bit-error rate (BER) of the proposed detection methods.

II. The CSK System

We consider a simple CSK system, in which the transmitter sends a signal consisting of chaotic signals extracted from two chaos generators. Essentially, the signal being transmitted toggles itself between the two sequences, $\{a_n\}$ and $\{b_n\}$, depending upon the value of the digital message to be sent, where n is the integer index for the sequence of values generated by the chaos generators, as shown in Fig. 1. In general, the two chaotic sequences are generated by two chaotic maps, f: $S \to S$ and g: $S \to S$ for $S \subset \Re$, s.t.

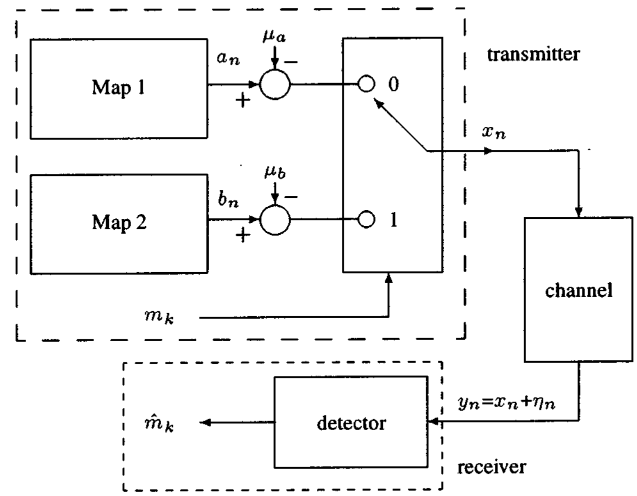

Fig. 1. Block diagram of the CSK system. m_k is the digital message and $\hat{m}_k$ is the restored message. μ_a and μ_b are the means of the chaotic signals a_n and b_n. η_n denotes white Gaussian noise.

$$\begin{cases} a_{n+1} = f(a_n) \\ b_{n+1} = g(b_n). \end{cases} \tag{1}$$

Now, consider the modulation process. Let m_k denote the kth bit, which is either "0" or "1." Also let N be the spreading factor, which is defined as the number of chaotic samples sent in one bit duration. The modulation proceeds as follows. In each bit duration, N consecutive values of either $\{a_n\}$ or $\{b_n\}$ are sent, depending upon the value of m_k. The output of the transmitter, x_n, during the kth bit duration, i.e., for $n = (k-1)N + 1, (k-1)N + 2, \ldots, kN$, is given by

$$x_n = \begin{cases} a_n - \mu_a, & \text{if } m_k = 0 \\ b_n - \mu_b, & \text{if } m_k = 1 \end{cases} \tag{2}$$

where μ_a and μ_b are the average values of the two chaotic sequences $\{a_n\}$ and $\{b_n\}$, respectively. Thus, the transmitter output, x_n, has a zero average. Further, assuming that the channel is subject to additive white Gaussian noise, the signal at the input to the receiver, y_n, is given by

$$y_n = x_n + \eta_n \tag{3}$$

where η_n is the added channel noise. At the receiving end, the general aim is to recover m_k with a minimum probability of error. Typical waveforms of transmitted signals are shown in Fig. 2. To avoid obscuring the essentials, we assume that the channel has sufficient bandwidth to permit the chaotic samples to be recovered in the receiving end. For instance, in the case of pulse-amplitude modulation (PAM), the required bandwidth should be at least half the sampling rate of the chaotic samples.

Manuscript received July 31, 2001; revised April 16, 2001. This work was supported by the Hong Kong Polytechnic under University Research Grant G-T418. This paper was recommended by Associate Editor T. Saito.

The authors are with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, (e-mail: encktse@polyu.edu.hk).

Digital Object Identifier 10.1109/TCSI.2002.803357.

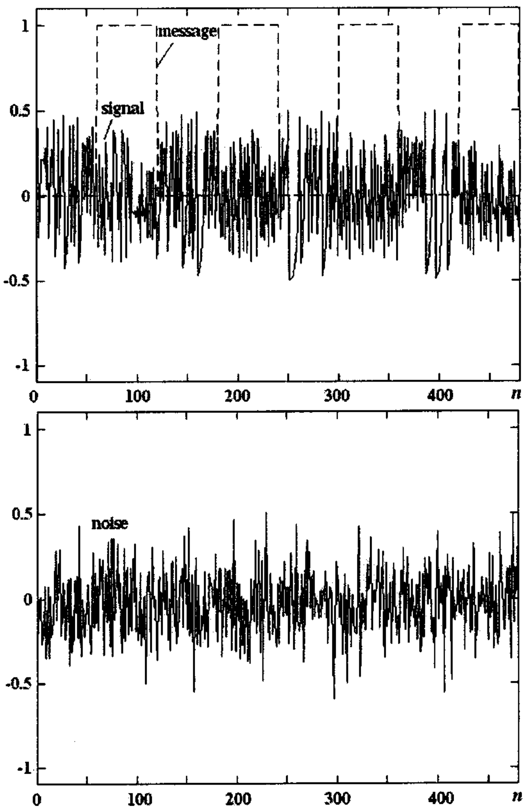

Fig. 2. Waveforms of (a) transmitted signal; (b) channel noise at $E_b/N_0 = 15$ dB. Message is "01 010 101…" and spreading factor is 60. Signals are generated from the tent maps, i.e., $f(x) = 1 - 2|x - (1/2)|$ and $g(x) = 2|x - (1/2)|$.

III. Non-Coherent Detection Based on Return Maps

In this section, we discuss specific detection approaches that make use of some deterministic property of the chaotic signals. Specifically, the return map will be exploited for detection, and two particular algorithms will be expounded. The first one is based on regression, and the second on maximizing the *a posteriori* probability. Fig. 3 shows a block diagram of the return-map-based detector.

A. Regression Approach

As mentioned previously, the CSK system involves two chaotic maps. In our proposed system, the chaotic maps are assumed to be written in a common form $h(.)$, with one distinguishing parameter p, i.e.

$$\begin{cases} \tilde{a}_{n+1} = h(p,\, \tilde{a}_n) \\ \tilde{b}_{n+1} = h\left(-p,\, \tilde{b}_n\right) \end{cases} \tag{4}$$

where $(\tilde{a}_n,\, \tilde{a}_{n+1})$ and $(a_n,\, a_{n+1})$ are related by a simple transformation T: $S^2 \to S'^2$, and so are $(\tilde{b}_n,\, \tilde{b}_{n+1})$ and $(b_n,\, b_{n+1})$. That is

$$(\tilde{a}_n,\, \tilde{a}_{n+1}) = T(a_n,\, a_{n+1}) \tag{5}$$

$$\left(\tilde{b}_n,\, \tilde{b}_{n+1}\right) = T(b_n,\, b_{n+1}). \tag{6}$$

As will become apparent, this requirement permits a simple regression procedure to be applied to the return map for effective detection. In particular, we consider the simple case where the parameter p appears explicitly as a multiplier to a common function $H(.)$, i.e.

$$\begin{cases} \tilde{a}_{n+1} = pH(\tilde{a}_n) \\ \tilde{b}_{n+1} = -pH\left(\tilde{b}_n\right). \end{cases} \tag{7}$$

As an example, consider the chaotic maps employing the tent maps $f(x) = 1 - 2|x - (1/2)|$ and $g(x) = 2|x - (1/2)|$ for all $x \in S = (0,\, 1)$. The corresponding common form is given by

$$H(x) = \tfrac{1}{2} - |2x| \tag{8}$$

and $p = 1$. Here, the transformed domain and range are $S' = (-(1/2),\, 1/2)$. See Fig. 4(a).

Likewise, for the logistic maps $f(x) = 4x(1-x)$ and $g(x) = 1 - 4x(1-x)$, with $S = (0,\, 1)$, the corresponding common form, with $S' = (-(1/2),\, 1/2)$, is

$$H(x) = \left(x - \frac{\sqrt{2}}{4}\right)\left(x + \frac{\sqrt{2}}{4}\right) \tag{9}$$

and $p = 4$ in this case. See Fig. 4(b).

The detection approach involves first collecting the points $(y_n,\, y_{n+1})$ for each bit. Then, the T transformation mentioned in the previous section is performed on these points, such that the resulting return map resembles either the curve $y = pH(x)$ or $y = -pH(x)$ under noise-free transmission, depending upon the transmitted bit m_k being "0" or "1." It should be noted that since the transmitter (as defined above) already removes the dc offset, the transformation may need to be adjusted to take into account the dc offset. For the two examples given above, no transformation is needed in the receiver because it is automatically done with the removal of the dc offset.

Under noisy conditions, the points on the collected and transformed return map appear scattered, but to a certain extent (depending upon the noise level) remain close to the curves $y = \pm pH(x)$. A typical reconstructed return map is shown in Fig. 5. Our detection is formulated on the basis of a regression algorithm which aims to find the best fit of the curve

$$y = q_k H(x) \tag{10}$$

to the points of the return map for the kth bit. The regression here is to estimate the parameter q_k such that the set of points is closest to the above curve in a least-square sense (see the Appendix). Once q_k is found, the decision rule can be as simple as

$$\hat{m}_k = \begin{cases} 0, & \text{if } q_k > 0 \\ 1, & \text{otherwise.} \end{cases} \tag{11}$$

Remarks: The essence of the transformation T is to allow the two chaotic maps to be written with *only one* parameter which "strongly" characterizes the map. If the map is written in terms of two or more parameters, then these parameters will jointly characterize the map. Thus, the estimated value of any one parameter may not provide sufficient characterization of the particular chaotic map in order to allow accurate decision to be made as to which map has been sent. Hence, with only one parameter characterizing the map, the detection can be more accurately done.

B. Probability Approach

In this subsection, we present an alternative approach for detection. The basis is still the return map, but the algorithm is based on maximizing the *a posteriori* probability.

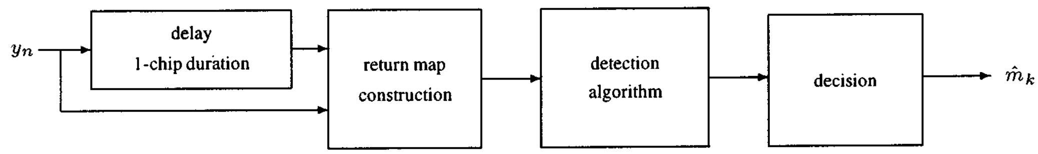

Fig. 3. Block diagram of the return-map-based detector.

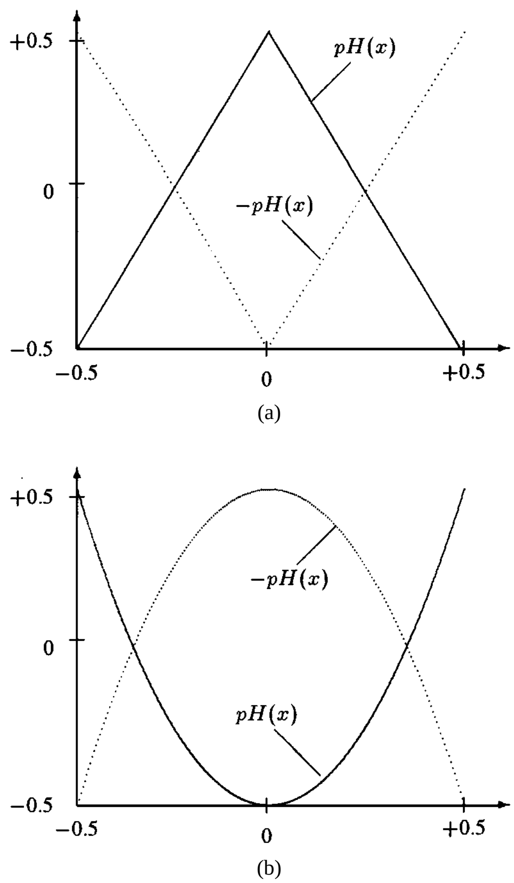

Fig. 4. Chaotic maps. (a) $H(x) = 0.5 - |2x|$, $p = 1$; (b) $H(x) = (x - \sqrt{2}/4)(x + \sqrt{2}/4)$, $p = 4$.

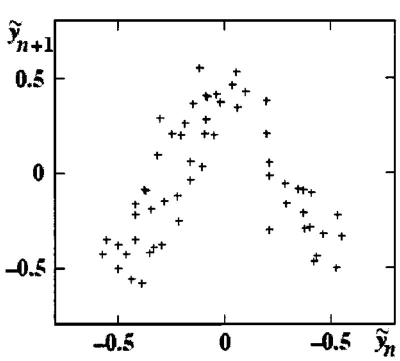

Fig. 5. Return map of received signal for symbol "0" at $E_b/N_0 = 25$ dB. Spreading factor is 60.

Without loss of generality, we consider the received signal for the first symbol, i.e., $k = 1$. For convenience of the subsequent description, we denote the received signal block for the first bit by $\boldsymbol{y} = (y_1 \;\; y_2 \;\; \cdots \;\; y_N)$, and define the observation vectors as $\boldsymbol{v}_i = (y_i \;\; y_{i+1})$ for $i = 1, 2, \ldots, N-1$. Define also $\boldsymbol{V} = (\boldsymbol{v}_1 \;\; \boldsymbol{v}_2 \;\; \cdots \;\; \boldsymbol{v}_{N-1})$. Note that this is simply the return map constructed for the first bit. We decode the incoming chaotic signal block by selecting the symbol that would maximize the *a posteriori* probability given $\boldsymbol{V}$, i.e.

$$\hat{m}_1 = \arg\max_{m_1} \mathrm{Prob}(m_1 \text{ is sent} \,|\, \boldsymbol{V}). \tag{12}$$

As the *a posteriori* probability is not convenient to calculate, the Bayes' rule is applied to $\mathrm{Prob}(m_1 \text{ is sent} \,|\, \boldsymbol{V})$ to obtain

$$\mathrm{Prob}(m_1 \text{ is sent} \,|\, \boldsymbol{V}) = \frac{p(\boldsymbol{V} \mid m_1 \text{ is sent})}{p(\boldsymbol{V})} \times \mathrm{Prob}(m_1 \text{ is sent}) \tag{13}$$

where $p(.)$ denotes the probability density function. Hence, (12) can be re-written as

$$\hat{m}_1 = \arg\max_{m_1} p(\boldsymbol{V}|m_1 \text{ is sent}) \tag{14}$$

because $\mathrm{Prob}(0 \text{ is sent}) = \mathrm{Prob}(1 \text{ is sent}) = 1/2$ and $p(\boldsymbol{V})$ is independent of m_1. In this detection scheme, we assume that $\boldsymbol{v}_i$ and $\boldsymbol{v}_j$ are independent for $i \neq j$. Thus, $p(\boldsymbol{V}|m_1 \text{ is sent})$ in (14) can be expressed as

$$p(\boldsymbol{V}|m_1 \text{ is sent}) = \prod_{i=1}^{N-1} p(\boldsymbol{v}_i|m_1 \text{ is sent}). \tag{15}$$

It should be pointed out that with this assumption, we effectively neglect the interdependence between the observation vectors, and thus the probability of an error occurring is expected to be larger than that of the optimal case studied by Hasler and Schimming [5], [6].

We also assume that in each of the observation vectors $\boldsymbol{v}_i = (y_i \;\; y_{i+1})$ $(i = 1, 2, \ldots, N-1)$, the initial condition of the chaotic signal s_i that gives rise to y_i is randomly selected from the chaotic range of the map according to the natural invariant probability density of the chaotic map. Now, suppose a "0" is sent, i.e., $m_1 = 0$, and the corresponding iterative map is f. Hence, we have

$$\begin{aligned}
&p(\boldsymbol{v}_i|0 \text{ is sent}) \\
&\quad = \int_{-\infty}^{\infty} p(\boldsymbol{v}_i|(0 \text{ is sent}, \, s_i))\rho_f(s_i)ds_i \\
&\quad = \int_{-\infty}^{\infty} \frac{1}{2\pi\sigma_n^2} \\
&\qquad \times \exp\left(-\frac{(y_i - s_i)^2 + (y_{i+1} - f(s_i))^2}{2\sigma_n^2}\right)\rho_f(s_i)\,ds_i \\
&\quad = \frac{1}{2\pi\sigma_n^2} \int_{-\infty}^{\infty} \rho_f(x) \\
&\qquad \times \exp\left(-\frac{(y_i - x)^2 + (y_{i+1} - f(x))^2}{2\sigma_n^2}\right)dx
\end{aligned} \tag{16}$$

where $\rho_f(x)$ and σ_n^2 denote the natural invariant probability density of f and variance of noise (noise power), respectively. Similarly, when a

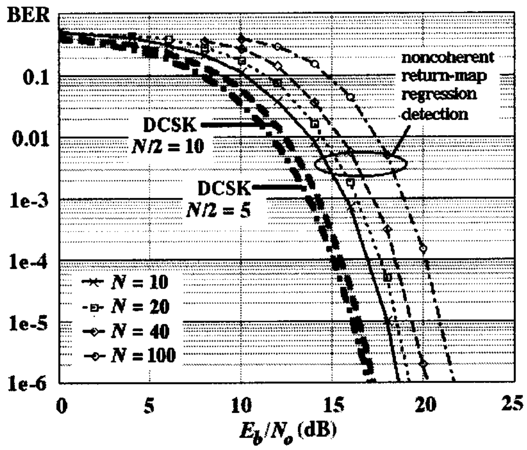

Fig. 6. BER (log scale) versus E_b/N_0 using the proposed regression-based detection. Spreading factor $N = 10$, 20, 40, and 100. Thick dash line corresponds to DCSK with $N/2 = 10$ which doubles the bandwidth requirement of our $N = 10$ case, and thick dot–dash line corresponds to DCSK with $N/2 = 5$ which requires same bandwidth as our $N = 10$ case.

"1" is sent and the corresponding iterative map is g, it is readily shown that

$$p(\boldsymbol{v}_i|1 \text{ is sent}) = \frac{1}{2\pi\sigma_n^2} \int_{-\infty}^{\infty} \rho_g(x) \times \exp\left(-\frac{(y_i - x)^2 + (y_{i+1} - g(x))^2}{2\sigma_n^2}\right) dx \tag{17}$$

where $\rho_g(x)$ represents the probability density of g. Note that since the transmitted signal contains no dc bias, the maps f and g should be chosen or translated appropriately such that they consistently contain no dc offset. The decision rule is simply given by

$$\hat{m_1} = \begin{cases} 0, & \text{if } \prod_{i=1}^{N-1} p(\boldsymbol{v}_i|0 \text{ is sent}) > \prod_{i=1}^{N-1} p(\boldsymbol{v}_i|1 \text{ is sent}) \\ 1, & \text{otherwise.} \end{cases} \tag{18}$$

The same detection algorithm applies to all other bits.

IV. Simulation Results and Comparisons

The performance of the proposed detection methods is evaluated by computer simulations. We use the simple tent maps [Fig. 4(a)] for chaos generation, and we present the BER of the system for a range of spreading factors. Results for the two cases, corresponding to the regression-based and probability-based algorithms, are presented separately. For consistency we adopt the usual definition of E_b/N_0 throughout the sequel, i.e.

$$\frac{E_b}{N_0} = \frac{\frac{1}{N_b}\sum_{n=1}^{N_bN} x_n^2}{\frac{2}{N_bN}\sum_{n=1}^{N_bN} \eta_n^2} = \frac{N}{2}\left(\frac{\sigma_s^2}{\sigma_n^2}\right) \tag{19}$$

where N_b is the number of bits simulated, N is the spreading factor (number of chips per bit), σ_s^2 is the signal power and σ_n^2 is the noise power.

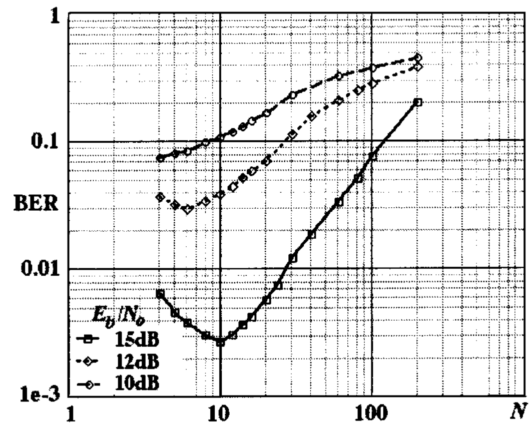

Fig. 7. Dependence of BER upon spreading factor N for the regression-based detector. The tent maps are used as chaos generators.

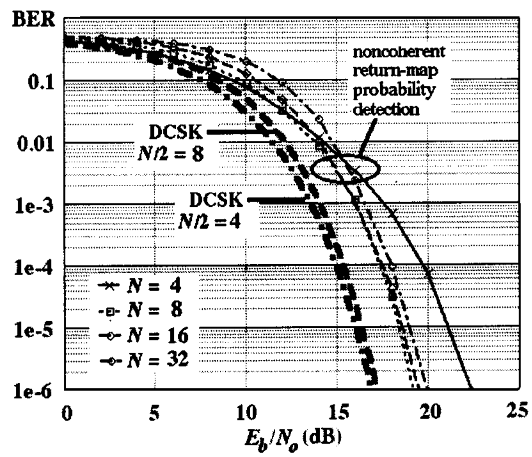

Fig. 8. BER (log scale) versus E_b/N_0 using the proposed probability-based detection. Spreading factor $N = 4$, 8, 16, and 32. The performance of the DCSK system is shown for comparison.

A. Regression Approach

For the regression-based detection, Fig. 6 shows the plots of the BER versus the usual E_b/N_0. For comparison we show the performance of the most widely studied noncoherent DCSK system with $N = 10$ and 20 [11], [12]. It is fairer to compare the DCSK system for $N = 20$ with our case for $N = 10$, since half of the chips in DCSK are used as reference, though the DCSK with $N = 20$ doubles the bandwidth requirement [13].

Next, we study the effect of varying the spreading factor N. From the simulation results, we may conclude that for constant E_b/N_0, the BER reaches a minimum for a certain spreading factor, as shown in Fig. 7. This behavior occurs typically in noncoherent detection and can be explained as follows. For small N, detection accuracy is poor due to insufficient data points. Thus, detection improves as N increases. However, as N increases, the noise level increases accordingly for constant E_b/N_0, causing deterioration of the performance. For small N, the advantage that can be gained from increasing data points is more significant than the corresponding deterioration due to increased noise level. However, for large N, the noise admitted becomes excessive, and the advantage that can be gained from increasing data points becomes insignificant, causing overall deterioration of the performance.

B. Probability Approach

The tent maps are again employed to generate the chaotic sequences. In Fig. 8, the BERs versus E_b/N_0 are shown. We observe that for

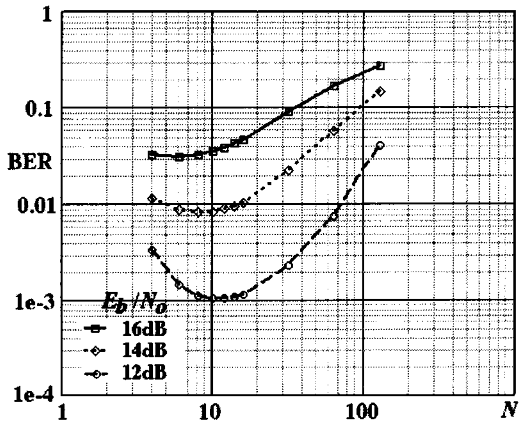

Fig. 9. Dependence of BER upon spreading factor N for the probability-based detector. The tent maps are used as chaos generators.

low E_b/N_0 values, using smaller spreading factors (e.g., 4 or 8) gives slightly better BER, whereas larger spreading factors produces comparatively lower BER for higher E_b/N_0. In Fig. 9, we plot the BERs versus the spreading factor in log scale. As in the regression-based detection method, for constant E_b/N_0, the BER achieves a minimum for a certain spreading factor. In this example, the minimum BERs are obtained with a spreading factor of about 10 for $E_b/N_0 = 12$, 14, and 16 dB.

It should be noted that the proposed detection methods represent only two particular possibilities of exploiting the return-map features, and they may not represent the most effective algorithm for detection. Nonetheless, our purpose is to demonstrate detection possibilities by suitably exploiting the chaotic determinism.

V. Conclusion

In this brief, we introduce methods for demodulating CSK signals, exploitating the built-in determinism of chaotic signals. We demonstrate in this brief, two methods exploiting the return maps for recovering the digital message carried by a CSK signal. The algorithm involves either a simple regression process or probability calculation. We conclude this brief by reiterating that methods based on detecting deterministic properties are still not exhausted and further improvement is possible for noncoherent detection based on this category of methods.

Appendix
Least Squares Estimate of Parameter

The basic problem in the regression approach is to fit a curve of the form $y = qH(x)$ to a set of data points (x_1, y_1), (x_2, y_2), ..., (x_n, y_n). The fitting objective is to minimize the residual sum of squares, defined as

$$\mathrm{SS} = \sum_{i=1}^{n} [y_i - qH(x_i)]^2$$

where q is the parameter to be estimated. From elementary calculus, we set the partial derivative of the residual sum of squares with respect to q to zero [14], i.e.

$$\frac{\partial \mathrm{SS}}{\partial q} = 0.$$

Expanding this, we get

$$\sum_{i=1}^{n} 2H(x_i)[y_i - (qH(x_i))] = 0.$$

The estimate of q is thus given by the following formula:

$$\hat{q} = \sum_{i=1}^{n} y_i H(x_i) \bigg/ \sum_{i=1}^{n} H(x_i)^2.$$

References

[1] H. Dedieu, M. P. Kennedy, and M. Hasler, “Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua’s circuit,” *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 634–642, Oct. 1993.

[2] H. Yu and H. Leung, “A comparative study of different chaos based spread spectrum communication systems,” in *Proc. IEEE Int. Symp. Circ. Syst.*, Sydney, Australia, May 2001, pp. III-213–216.

[3] C. C. Chen and K. Yao, “Stochastic-calculus-based numerical evaluation and performance analysis of chaotic communication systems,” *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1663–1672, Dec. 2000.

[4] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, “Performance analysis of correlation-based communication schemes utilizing chaos,” *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1684–1691, Dec. 2000.

[5] M. Hasler and T. Schimming, “Chaos communication over noisy channels,” *Int. J. Bifurcation Chaos*, vol. 10, no. 4, pp. 719–735, 2000.

[6] F. C. M. Lau and C. K. Tse, “Approximate-optimal detector for chaos communication systems,” *Int. J. Bifurcation Chaos*, to be published.

[7] G. Kolumbán, “Theoretical noise performance of correlator-based chaotic communication schemes,” *IEEE Trans. Circuits Syst. I*, vol. 47, no. 12, pp. 1692–1702, Dec. 2000.

[8] G. Kolumbán, M. P. Kennedy, and L. O. Chua, “The role of synchronization in digital communication using chaos—Part I: Fundamentals of digital communications,” *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 927–936, Oct. 1997.

[9] M. P. Kennedy and G. Kolumbán, “Digital communication using chaos,” in *Controlling Chaos and Bifurcation in Engineering Systems*, G. Chen, Ed. Boca Raton, FL: CRC Press, 2000, pp. 477–500.

[10] T. Schimming and M. Hasler, “Optimal detection of differential chaos shift keying,” *IEEE Trans. Circuits Syst. I*, vol. 47, pp. 1712–1719, Dec. 2000.

[11] G. Kolumbán, B. Vizvari, W. Schwarz, and A. Abel, “Differential chaos shift keying: a robust code for chaos communication,” in *Proc. Int. Spec. Workshop Nonlinear Dynamics Electron. Syst.*, Seville, Spain, June 1996, pp. 87–92.

[12] A. Abel, M. Gotz, and W. Schwarz, “Statistical analysis of chaotic communication schemes,” in *Proc. IEEE Int. Symp. Circuits Systems*, Monterey, CA, May 1998, pp. 465–468.

[13] A. Kisel, H. Dedieu, and T. Schimming, “Maximum likelihood approaches for noncoherent communications with chaotic carriers,” *IEEE Trans. Circuits Syst. I*, vol. 48, pp. 533–542, May 2001.

[14] R. J. Freund and W. J. Wilson, *Regression Analysis: Statistical Modeling of a Response Variable*. San Diego, CA: Academic, 1998.