Available online at www.sciencedirect.com
SCIENCE DIRECT®
Physics Letters A 334 (2005) 30–36
PHYSICS LETTERS A
www.elsevier.com/locate/pla

Spread-spectrum communication using binary spatiotemporal chaotic codes

Xingang Wang [a,*], Meng Zhan [a], Xiaofeng Gong [a], Choy Heng Lai [b], Ying-Cheng Lai [c]

[a] *Temasek Laboratories, National University of Singapore, Singapore 117508, Singapore*
[b] *Department of Physics, National University of Singapore, Singapore 117542, Singapore*
[c] *Department of Mathematics and Statistics, Departments of Electrical Engineering and Physics, Arizona State University, Tempe, AZ 85287, USA*

Received 15 September 2003; received in revised form 12 October 2004; accepted 26 October 2004

Available online 12 November 2004

Communicated by A.P. Fordy

Abstract

We propose a scheme to generate binary code for baseband spread-spectrum communication by using a chain of coupled chaotic maps. We compare the performances of this type of spatiotemporal chaotic code with those of a conventional code used frequently in digital communication, the Gold code, and demonstrate that our code is comparable or even superior to the Gold code in several key aspects: security, bit error rate, code generation speed, and the number of possible code sequences. As the field of communicating with chaos faces doubts in terms of performance comparison with conventional digital communication schemes, our work gives a clear message that communicating with chaos can be advantageous and it deserves further attention from the nonlinear science community.

PACS: 05.45.Vx; 05.45.-a

Keywords: Spatiotemporal chaos; Chaos synchronization; Spread-spectrum communication; Pseudo-random code generator

The field of communicating with chaos starts with the work of Pecora and Carroll on synchronization in chaotic systems [1] and that of Hayes et al. on encoding information using symbolic dynamics [2,3]. Since then there has been a tremendous amount of effort in this area in the hope that a new communication scheme may arise with potential for implementation in realistic applications. Representative works include that by Kocarev et al. who used the idea of masking to hide information in chaotic signals [4], by Cuomo and Oppenheim who demonstrated that a message can indeed be transmitted by using chaotic synchronization [5], and by Parlitz et al. who considered chaotic modulation in combination with the traditional spread-

* Corresponding author.
E-mail address: tslwxg@nus.edu.sg (X. Wang).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2004.10.075

spectrum communication technique for transmitting binary information [6,7]. The important issue of security was also considered [8–16]. In terms of the symbolic dynamics approach [2,3], various schemes were proposed and the nonlinear dynamics of the coding process were studied [17–20]. For recent progress, see Ref. [21].

As conventional digital communication technologies have become fairly advanced and widespread, a burning issue facing researchers in communicating with chaos is how it compares with the existing schemes in terms of performances. The purpose of this Letter is address one issue that is essential to any digital communication scheme, conventional or chaos-based: pseudo-random code generation. Conventionally, code generation is accomplished by using linear shift-register generators that generate binary sequences such as the Gold code for spread-spectrum communication [22]. Such sequences are pseudo-random, and the idea is to convolute the sequences with the wave signal that carries the information to be transmitted. At the receiver, the original information is recovered by a despreading process, which is achieved by correlating the received spread signal with a synchronized replica of the code signal. Because of the pseudo-randomness of the code, the transmitting signal usually has a bandwidth that is much greater than the minimum bandwidth necessary to send the information, rendering the signal secure and noise-resistant. This spread-spectrum technique has become the cornerstone of many modern digital communication systems, including the global positioning systems [23]. As we can see, the key to spreading the spectrum of the communication signal is a proper pseudo-random code.

In this Letter, we propose a scheme based on a class of spatio-temporal chaotic dynamical systems to generate pseudo-random code for spread-spectrum communication. In particular, we use a chain of unidirectionally coupled chaotic maps [24,25] to generate binary code sequences. This type of coupled-map system was originally proposed for encryption of information but here we address the problem of code generation for spectrum spreading. We choose the system because it has fast speed and robust synchronization properties, thereby being capable of facilitating the final despreading process at the receiver end. We shall present analysis and numerical evidence that our spatio-temporal chaotic code can be comparable or even superior to conventional pseudo-random codes such as the Gold code in several key aspects: security, bit error rate, code generation speed, and the number of possible code sequences. Since these results have been obtained by comparing our code directly and quantitatively with the Gold code, they are encouraging in the sense that they may help reinforce the speculation that chaos-based communication schemes can be advantageous, a belief that stimulated many works on communicating with chaos in the nonlinear-science community.

We use the following class of unidirectionally coupled chaotic maps to generate binary codes:

$$x_i(n+1) = (1-\varepsilon_i) f\big[x_i(n)\big] + \varepsilon_i f\big[x_{i-1}(n)\big], \quad i = 1, 2, \ldots, m, \tag{1}$$

where m is the number of coupled maps, $f(x) = 4x(1-x)$ is the chaotic logistic map, and ε_i is the coupling strength that can potentially be used as the secret keys for secure communication [26,27]. While both space and time are discrete in Eq. (1), the dynamical variables x_i are continuous. Given $x_i(n)$, to generate a sequence of binary numbers $K^i(n)$, we use the following procedure:

$$M^i(n) = \text{int}\big[x_i(n) \times 10^{\mu}\big] \bmod \big(2^{\nu}\big),$$
$$K^i(n) = \text{binary}\big[M^i(n)\big], \tag{2}$$

where ν is the number of bits of the source information, and μ is an integer chosen such that 10^{μ} is on the order of the inverse of the computer precision. The boundary condition is given by $x_0(n) = K(n)/2^{\nu}$, where $K(n) = \text{int}[x_m(n) \times 10^{\mu}] \bmod (2^{\nu})$. We see that $M^i(n)$ represents the number of insignificant digits of $x_i(n)$ and $K^i(n)$ is simply the binary version of $M^i(n)$. For a given coupled-map lattice, Eq. (2) generates, for each map, ν bits of binary data at each iteration. Regarding each map as a code generator, a lattice of m coupled maps thus represents a parallel set of m code generators. This is shown schematically in Fig. 1. For spread-spectrum communication, each user can be assigned a map in the lattice, and each code sequence K^i $(i = 1, \ldots, m)$ of length N can be used as a basis function for modulation (in general, a basis is constructed by several iterations since each iteration only contributes ν bit codes for each lattice). A possible modulation scheme can be, for instance, as

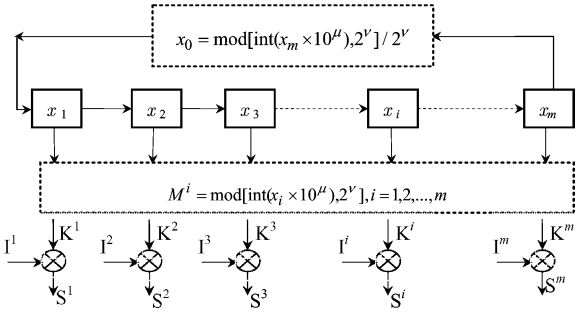

Fig. 1. Black diagram of the binary spatiotemporal chaotic code generator.

follows: if the binary information bit to be transmitted is $I^i = 1$, the modulated bit is $S^i = K^i$, while if $I^i = 0$, $S^i = -K^i$ is chosen.

To recover the transmitted information on the receiver end, an identical chain of synchronized coupled maps is needed. For simplicity, at the first step, we assume that the transmitter and receiver are synchronized by having the same parameters and initial conditions. Binary information can be recovered by the process of coherent demodulation using correlators at the receiver end [22]. In our coupled-map lattice scheme, each lattice site on the receiver end can actually be regarded as a correlator.

Some basic properties of a pseudo-random code are auto- and cross-correlations, balance, run-length distribution, and frequency spectrum. We now discuss these properties for our chaotic code. (1) Given two binary sequences $K^i(N)$ and $K^j(N)$, the auto- and cross-correlations are defined, respectively, as follows:

$$C_{ii}(\tau) = \frac{\sum_{l=1}^{N} K^i(l)K^i(l+\tau)}{\sum_{l=1}^{N}[K^i(l)]^2} \quad \text{and}$$
$$C_{ij}(\tau) = \frac{\sum_{l=1}^{N} K^i(l)K^j(l+\tau)}{\sum_{l=1}^{N}[K^i(l)]^2}. \tag{3}$$

In general, it is desirable to have as small values as possible for the correlations (except for $\tau = 0$ in the autocorrelation) to ensure security and to overcome interferences in a multi-user environment. As shown in Fig. 2(a) and (b), our chaotic codes have these desirable properties, where in the simulation, codes with length of $N = 2^7 - 1$ bits are used. (2) The balance property measures the probability for observing zero (or one) in a code which, in the ideal case, should be $1/2$ so that the codes are as random as possible. Simulation results of the two probabilities for zero and one are shown in Fig. 2(c), where we see that as the code length is increased, both probabilities approach $1/2$. (3) For a purely random binary sequence, the probability for observing a symbol consecutively L times decreases with L according to 2^{-L}. Our chaotic binary code actually possesses this property, as shown in Fig. 2(d). (4) Finally, the power spectral density of a purely random sequence has the following form [28]:

$$S(f) = t\left(\frac{\sin \pi f t}{\pi f t}\right)^2, \tag{4}$$

where t is the actual time duration of one bit of code sequence. Fig. 3 shows an example of the power spectral density of a chaotic binary code, where $t = 1/N$ and $N = 2^{14}$ is the length of the example sequence. For comparison, the density $S(f)$ in Eq. (4) is also plotted (the upper trace). We see that the density of our chaotic code follows closely that of a purely random sequence. These results suggest that chaotic codes generated by coupled map lattices satisfy the basic requirements for secure, spread-spectrum communication.

We now consider a multi-user environment, where interference and noise are the major sources of error in a spread-spectrum communication [22], and demonstrate that the error performance of our chaotic binary sequences is comparable to the Gold code that is considered optimal and used commonly in many modern digital communication systems. Let $S^u(t)$ be the pulse-amplitude modulation information signal of the uth user:

$$S^u(t) = \sum_{s=0}^{\infty} S_s^u g_T(t - sT),$$

where $S_s^u \in \{-1, +1\}$ are the binary symbols that encode the information, g_T is a rectangular pulse which is 1 within $[0, T]$ and 0 outside, and T is the duration of each information bit. Suppose N is the length of the binary sequence used to modulate one information bit. With binary sequences y_l^u $(l = 1, \ldots, N)$ generated by Eqs. (1) and (2), we can construct the spreading basis:

$$Q^u(t) = \sum_{s=0}^{\infty} Q_s^u(t) g_T(t - sT) \quad \text{with}$$
$$Q_s^u(t) = \sum_{l=sN+1}^{(s+1)N} y_l^u g_{T/N}\left(t - l\frac{T}{N}\right), \tag{5}$$

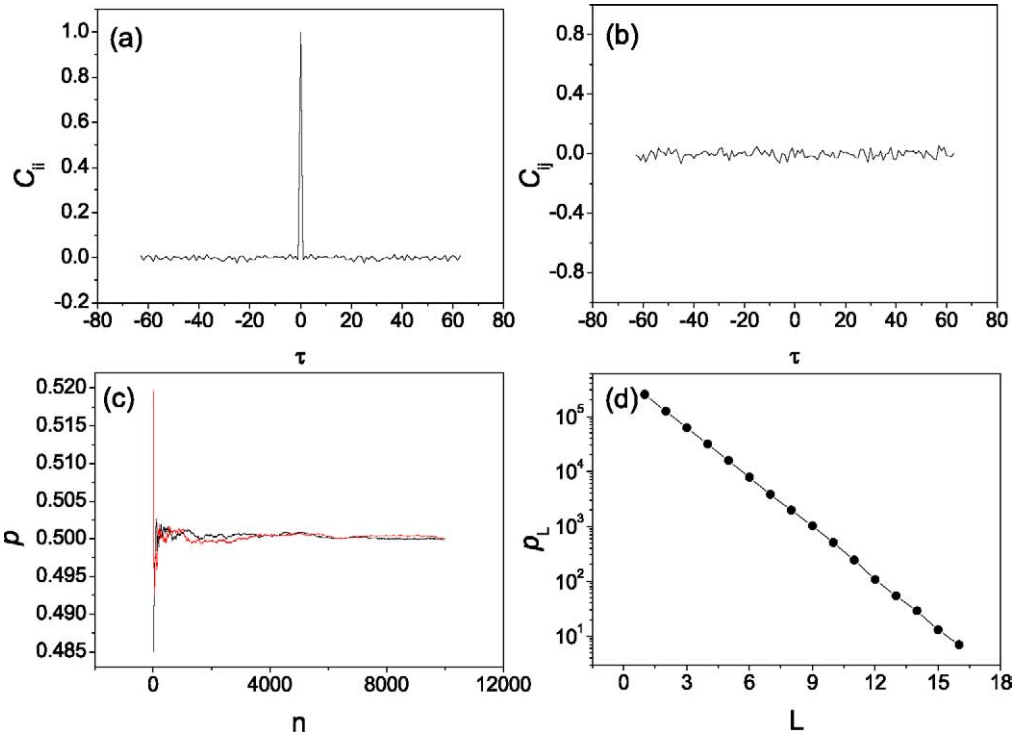

Fig. 2. For the chaotic code generator Eqs. (1) and (2) with $\mu = 10$ and $\nu = 6$, (a), (b) autocorrelation and cross-correlation of binary sequences of length $N = 2^7 - 1$ bits, respectively. The results were averaged using 10 realizations. (c) Probabilities of observing the numbers of 0 and 1 in a binary code (the balance property), and (d) exponential decay in the probability to observe a number of consecutive zeros (the run-length distribution). All indicate that chaotic codes are comparable to classical codes in terms of the basic properties required for spread-spectrum communication.

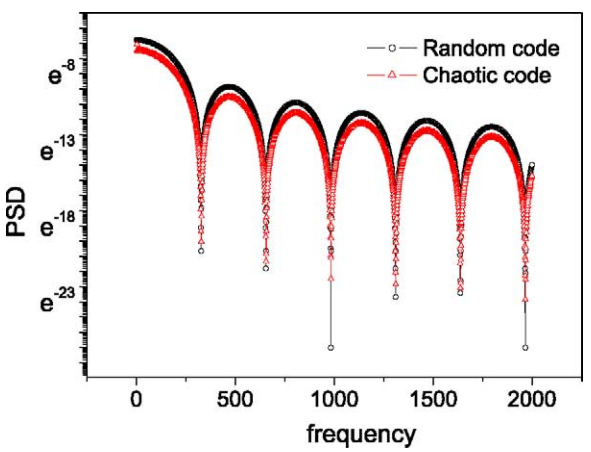

Fig. 3. For Eqs. (1) and (2) with $\mu = 10$ and $\nu = 6$, a typical power spectral density of the generated chaotic code (the lower trace). Also shown is the density from a purely random sequence (the upper trace).

where $g_{T/N}$ is 1 within $[0, T/N]$ and 0 outside, l is the location of the bits in the spreading sequence. The output spreading signal for symbol S_s^u can be written as

$$S_s^u(t) = S_s^u Q_s^u(t) = \sum_{l=sN+1}^{(s+1)N} S_s^u y_l^u g_{T/N}\left(t - l\frac{T}{N}\right). \quad (6)$$

In the simple case where there is only a single-user and noise is absent, the symbol S_s^u can be recovered at the receiver end by correlating $S_s^u(t)$ with the same basis $Q_s^u(t)$:

$$\Phi_s^u = \frac{1}{T}\int_{sT}^{(s+1)T} Q_s^u(t) S_s^u(t)\,dt = S_s^u \sum_{l=sN+1}^{(s+1)N} \left|y_l^u\right|^2 = N S_s^u. \quad (7)$$

In a multi-user environment, the interference caused by the vth user at the uth receiver is

$$\Psi_s^{uv} = \frac{1}{T}\int_{sT}^{(s+1)T} Q_s^v(t)S_s^u(t)\,dt = S_s^u \sum_{l=sN+1}^{(s+1)N} y_l^u y_l^v. \tag{8}$$

Say there are U users sharing the same channel. Since the binary chaotic sequences generated are random in practical time scales that are typically much longer than the correlation time of the underlying chaotic process, the interference term acting on the uth user can be regarded as a sum of zero mean, independent random variables [29]:

$$\left(\sigma^u\right)^2 = E\left[\left(\Psi_s^u\right)^2\right] = E\left[\left(\sum_{v\neq u, v=1}^{U} \Psi_s^{uv}\right)^2\right], \tag{9}$$

where $E[.]$ is the mean value of all symbols transmitted. Since the signal-to-interference ratio for the uth user is proportional to $(\Phi_s^u/\sigma^u)^2$, by choosing 0 as the decision criterion we can write the bit-error-rate as

$$P_{\text{err}} = Q\left(\Phi_s^u/\sigma^u\right), \tag{10}$$

where $Q(x) = 1/\sqrt{2\pi}\int_x^\infty e^{-y^2/2}\,dy$ is the error function. In the presence of noise, the bit error rate becomes

$$P_{\text{err}} = Q\left[\Phi_s^u/\left(\sigma^u + \sigma\right)\right], \tag{11}$$

where σ is the variance of the additive Gaussian white noise.

Eq. (9) indicates that the variance of multi-user interference becomes large as the number of users is increased. Fig. 4(a) shows, for $N = 2^7 - 1$ and $m = 60$ in Eq. (1), the bit error rate as a function of the number (U) of users. For comparison, we plot the same relation but for the classical Gold sequences generated using a 25-stage linear shift register generators.[1] We see that the differences between the bit error rates in our chaotic sequences and Gold sequences are insignificant for small values of U and neglectable for large values of U, suggesting that our chaotic code sequences can perform almost as well as the Gold sequence in terms of the bit error rate in a multi-user environment. This result is further strengthened by simulation result of the bit error rate versus the signal-to-noise ratio, as shown in Fig. 4(b) for four representative values of U. For each value of U, two data sets are plotted, the lower one from the Gold code and the upper one from the chaotic code. We see that the differences in the bit error rate between the two codes are small, as desired.

While chaotic signals possess a number of properties typically associated with random signals, which makes chaotic codes suitable for spread-spectrum communication, the issue of synchronizability may be of concern. Without drivering signals, any mismatch in the initial conditions will cause desynchronization events. Even under self-synchronous schemes, for chaotic systems, the synchronization time may be very long and often induces a high bit error rate in practice, which can be particularly serious for high-dimensional chaotic systems. Fortunately, for our system (1), because of the uni-directionally coupled map lattices scheme, these difficulties can be alleviated, as previous work demonstrated that fast and robust synchronization can be achieved when the coupling strength exceeds a reasonable amount [30]. For instance, we have found in our simulation that for two systems given by Eq. (1), one acting as a transmitter and another as a receiver, the synchronization time is typically within

[1] A Gold code is constructed using two maximum-length sequences (m-sequences). Briefly, an m-sequence can be generated by using a simple linear shift register generator that has all the feedback signals returned to a single input of a shift register, or a delay line. Given a set of feedback connection coefficients $(c_1, \ldots, c_n)$, where c_i is chosen to be either 0 (open) or 1 (connect), the sequence a_i (0 or 1) is generated according to the recursive formula: $a_i = c_1 a_{i-1} + c_2 a_{i-2} + \cdots + c_n a_{i-n} = \sum_{k=1}^{n} c_k a_{i-k} \bmod (2)$, where all terms are binary (0 or 1). The sequence so generated is pseudo-random in the sense that the period (or length) of the sequence is $2^n - 1$. The m-sequence codes, while convenient to generate, are not secure because they are linear. In addition, the crosscorrelation between independently generated m-sequences typically has large values and, hence, they are not usable in a multi-user environment. To overcome these difficulties, the Gold codes are used, which are product codes achieved by the exclusive or-ring with modulo-2 adding of two m-sequences. The code sequences are added bit by bit by synchronous clocking. In general, a large number of Gold codes with the same length and with controlled cros-scorrelation can be generated. For mathematical details of m-sequences and Gold codes, see Ref. [22].

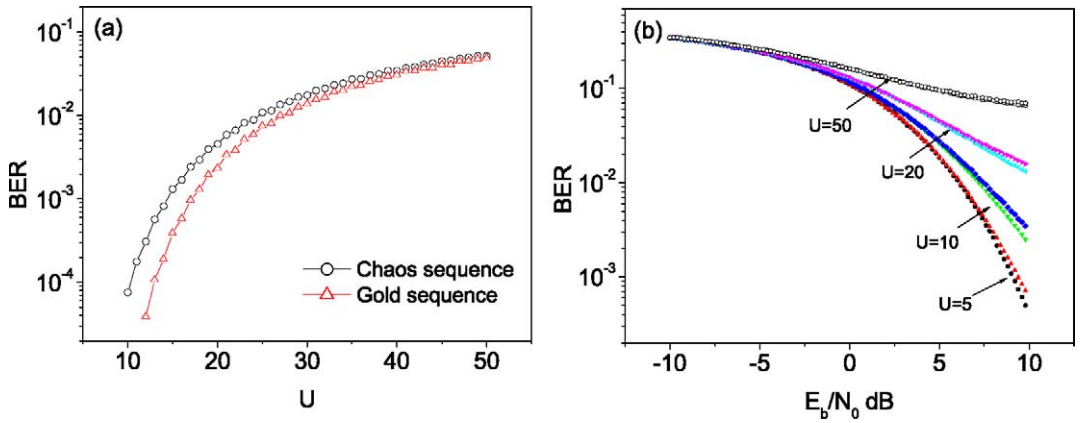

Fig. 4. For Eqs. (1) and (2) with $\mu = 10$, $\nu = 6$, and $N = 2^7 - 1$, (a) bit error rate versus the user number in a multi-user and noiseless environment, and (b) bit error rate versus the signal-to-noise ratio in a multi-user and noisy environment. Also shown in both panels are the corresponding plots from the classical Gold code.

150 iterations for $\epsilon = 0.95$ and $m = 60$. To transmit the driving signal for synchronization, the spreading method can again be used. For instance, from the last map site in the transmitter system one can obtain a binary sequence $K^m(n)$, as in Eq. (2). This binary sequence can be transmitted as information bits by some standard spreading method such as one utilizing the Gold code. The binary sequance can be converted into a continuous signal at the receiver, and then be used to synchronize the receiver system. Once synchronization between the transmitter and the receiver is established, spread-spectrum communication using chaotic codes can then be recovered.

In comparison with classical codes, chaotic codes not only have comparable performance in dealing with multi-user interference and noise disturbance, but also have some special properties superior to the former. Firstly, classical codes generated by linear shift register generators are easily decipherable once a short sequential set of bits ($2n + 1$ with n being the number of generator stages) from the sequence is known. In contrast, security of the modified spatiotemporal chaotic model, Eqs. (1) and (2), has been identified to be extremely high, even higher than the new issued advanced encryption standard [15,16,20,27]. Secondly, for an m-stage linear shift register generator, the number of maximum length sequences is given by $\psi(2^m - 1)/m$, where ψ is the Euler's totient function, and for each preferred pair m-sequences, the total number of the Gold sequences is only $2^m - 1$ [22]. In constrast, for the coupled map system (1), any change of the initial conditions or parameters will generate m new sequences. Since both the initial conditions and the parameters are real values and can be chosen randomly in certain ranges, theoretically there are an infinite number of sequences that can be generated. Furthermore, for each system there are a total of m generators working in parallel, and this can greatly improve the code generating speed. We also find that ν, the number of bits in a code, has little influence on the properties and performance of the codes. It is thus possible to generate a large number of codes at fast speed.

A shortcoming of the chaotic communication scheme proposed in this Letter is that the transmitter and the receiver must be highly synchronizable, which stipulates that the two systems be nearly identical. While synchronization time can be shortened by using more significant digits rather than the least significant ones in generating the driving signal, the security of the communication may be compromised. In practice, there is then a tradeoff between the synchronization speed and the degree of security. In this regard, improvements based on model selection and coupling schemes may help [26].

In conclusion, we have proposed a code generation scheme based on spatiotemporal chaos in a coupled-map lattice system, and demonstrated the potential to use the codes for baseband spread-spectrum communication. The random nature and the properties of the codes in terms of spread-spectrum communication criteria are analyzed. In addition to being able to match some commonly used classical codes in several key

properties, our chaotic codes can be more secure and be generated at high speed in large numbers. These results suggest that chaotic codes can be practically useful for digital spread-spectrum communication.

Acknowledgements

Y.-C.L. acknowledges the great hospitality of National University of Singapore, where part of this work was done during a visit. Y.-C.L. also wishes to acknowledge the support from AFOSR under Grant No. F49620-03-1-0290.

References

[1] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[2] S. Hayes, C. Grebogi, E. Ott, Phys. Rev. Lett. 70 (1993) 3031.
[3] S. Hayes, C. Grebogi, E. Ott, A. Mark, Phys. Rev. Lett. 73 (1994) 1781.
[4] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, Int. J. Bifur. Chaos Appl. Sci. Engrg. 2 (1992) 709.
[5] K.M. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[6] U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle, A. Shang, Int. J. Bifur. Chaos Appl. Sci. Engrg. 2 (1992) 973.
[7] U. Parlitz, S. Ergezinger, Phys. Lett. A 188 (1994) 146.
[8] G. Heidari-Bateni, C.D. McGillem, IEEE Trans. Commun. 42 (1994) 1524.
[9] G. Perez, H.A. Cerdeira, Phys. Rev. Lett. 74 (1995) 1970.
[10] K.M. Short, A.T. Parker, Phys. Rev. E 58 (1998) 1159.
[11] C. Zhou, C.-H. Lai, Phys. Rev. E 60 (1999) 320.
[12] F. Dachselt, W. Schwarz, IEEE Trans. Circuits Systems I Fund. Theory Appl. 48 (2001) 1498.
[13] L. Kocarev, IEEE Circuits Syst. Magz. 1 (2001) 6.
[14] B. Fraser, P. Yu, T. Lookman, Phys. Rev. E 66 (2002) 017202.
[15] S.H. Wang, J. Kuang, J. Li, Y. Luo, H. Lu, G. Hu, Phys. Rev. E 66 (2002) 065202.
[16] G. Tang, S. Wang, H. Lu, G. Hu, Phys. Lett. A 318 (2003) 388.
[17] E. Bollt, M. Dolnik, Phys. Rev. E 55 (1997) 6404.
[18] E. Bollt, Y.-C. Lai, C. Grebogi, Phys. Rev. Lett. 79 (1997) 3787.
[19] Y.-C. Lai, E. Bollt, C. Grebogi, Phys. Lett. A 255 (1999) 75.
[20] M. Baptista, C. Grebogi, E.E. Macau, Y.-C. Lai, E. Rosa, Phys. Rev. E 62 (2000) 4835.
[21] J. Kurths, S. Boccaletti, C. Grebogi, Y.-C. Lai, Chaos 13 (2003) 126.
[22] R.C. Dixon, Spread Spectrum Systems, second ed., Wiley, New York, 1984.
[23] B. Hofmann-Wellenhof, H. Lichtenegger, J. Collins, Global Positioning System: Theory and Practice, fifth ed., Springer-Verlag, Berlin, 2001.
[24] J.H. Xiao, G. Hu, Z.L. Qu, Phys. Rev. Lett. 77 (1996) 4162.
[25] X. Yongxiang, S. Xiuming, R. Yong, Y. Xunhe, L. Feng, Phys. Rev. E 64 (2001) 067201.
[26] X.G. Wang, M. Zhan, C.H. Lai, G. Hu, Chaos 14 (2004) 128.
[27] H. Lu, S. Wang, X. Li, G. Tang, J. Kuang, W. Ye, G. Hu, Chaos 14 (2004) 617.
[28] B. Sklar, Digital Communications: Fundamentals and Applications, Prentice–Hall, Englewood Cliffs, NJ, 1988.
[29] G. Mazzini, G. Setti, R. Rovatti, IEEE Trans. Circuits Systems I Fund. Theory Appl. 45 (1998) 496.
[30] G. Hu, J. Xiao, J. Wang, F. Xie, Z. Qu, Phys. Rev. E 56 (1997) 2738.