Hindawi Publishing Corporation
Discrete Dynamics in Nature and Society
Volume 2015, Article ID 818421, 11 pages
http://dx.doi.org/10.1155/2015/818421

Research Article

A Proposed Chaotic-Switched Turbo Coding Design and Its Application for Half-Duplex Relay Channel

Tamer H. M. Soliman, Fengfan Yang, and S. Ejaz

College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

Correspondence should be addressed to Tamer H. M. Soliman; thms78@gmail.com

Received 31 December 2014; Revised 26 March 2015; Accepted 29 March 2015

Academic Editor: Daniele Fournier-Prunaret

Both reliability and security are two important subjects in modern digital communications, each with a variety of subdisciplines. In this paper we introduce a new proposed secure turbo coding system which combines chaotic dynamics and turbo coding reliability together. As we utilize the chaotic maps as a tool for hiding and securing the coding design in turbo coding system, this proposed system model can provide both data secrecy and data reliability in one process to combat problems in an insecure and unreliable data channel link. To support our research, we provide different schemes to design a chaotic secure reliable turbo coding system which we call chaotic-switched turbo coding schemes. In these schemes the design of turbo codes chaotically changed depending on one or more chaotic maps. Extensions of these chaotic-switched turbo coding schemes to half-duplex relay systems are also described. Results of simulations of these new secure turbo coding schemes are compared to classical turbo codes with the same coding parameters and the proposed system is able to achieve secured reasonable bit error rate performance when it is made to switch between different puncturing and design configuration parameters especially with low switching rates.

1. Introduction

The demand for reliable and secure high data rates transmission over wireless links has been accelerated by the emergence of large-scale commercial communication networks and many military applications. One of the possible methods to provide security and reliability in a communication system without any increase in computational complexity is to embed security in channel-coding techniques. So, merging error correction techniques and security in a single block is an important aspect especially in a public and unreliable noisy channel.

Chaos is a universal phenomenon found in a wide spectrum of natural phenomena and nonlinear systems. The start of a positive relationship between chaotic systems and cryptography has been pointed out [1–5]. Chaotic systems present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates and excellent security. Chaos is characterized by the way that the dynamical system does not repeat itself, even though the system is governed by deterministic equations, meaning that their future dynamics are fully defined by its initial conditions. Chaotic applications became a hot topic in secrecy communication and engineering because chaotic signals were considered to provide good properties for a lot of applications.

Several schemes for applying the nonlinear dynamics of the chaotic systems to enhance the security of a communication system have been proposed [6–16]. A lot of research work on combining error correction codes and chaos in communication systems has been done [17, 18], while the authors in [19–21] proposed a combining chaotic turbo coding system into a single processing step in order to reduce the processing time and complexity. Combining error correction and cryptographic schemes in communication has been addressed in [22–24]. The concept of combining chaotic switching with error correction codes appeared in [18], but in this work the author designed a channel-coding scheme that combines a convolutional codec and a chaotic system. But due to the good error performance of turbo codes [25], which is closed to the Shannon Limit, we design new secured and reliable schemes that combine turbo code with chaotic

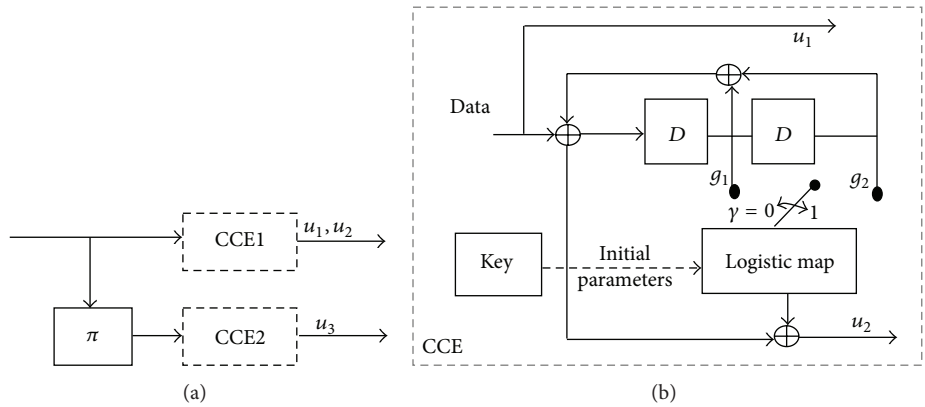

Figure 1: Chaotic-switched turbo code system. (a) Parallel concatenated CSTC and (b) CCE encoder design example.

system dynamics into a single step. The rate of turbo code is a very important parameter in the encoder design which can be considered as a switched parameter that can control the turbo encoder output.

In this work, we propose new efficient chaos secured turbo coding schemes based on using chaotic maps as a switching element to chaotically control the turbo encoder output. The architecture of the proposed chaotic-switched turbo code is based on designing a new coding scheme that possesses both the capabilities of error correction and encryption. The advantages of our schemes are that they can achieve secure reliable system performances by combining the turbo coding properties with chaos dynamics using different chaotic maps without requiring classical encryption techniques. Firstly, we explain the design of the proposed chaotic switching schemes. Secondly, the comparison between the proposed system schemes performance and the conventional turbo code are done by simulation. Finally, we extend this work further to two different cooperative receive diversity turbo coding scenarios: (1) chaotic cooperative multiple turbo code scheme and (2) the use of chaotic distributed turbo code scheme. For both scenarios, we consider a half-duplex decode and forward relaying system.

The paper is organized as follows. In Section 2, we present the chaos turbo code schemes. The first chaotic-switched turbo code (CSTC) scheme is designed using one-dimension (1D) logistic map and the second scheme of chaotic punctured switched turbo code (CPSTC) is designed on using the tent map. Also in this section, the use of coupled chaotic maps as a switching element in turbo coding design is introduced. The simulation of all chaos turbo code schemes is done in Section 3. We extend our work of the chaos switched turbo coding/decoding schemes for the relay channel in Section 4, and we conclude the paper in Section 5.

2. Proposed Chaos Turbo Coding Schemes

2.1. Chaotic-Switched Turbo Codes. Since it is possible to apply the chaos system in the hidden communication process only when the subsystems are synchronized, we assume in our schemes that the decoder is chaotically synchronized with the encoder. As the basic construction of classical turbo encoder by Berrou et al. [25], the CSTC system shown in Figure 1(a) consists of two main concatenated chaotic convolution encoders (CCE). The design of each CCE is introduced in Figure 1(b) where we adjust the chaotic switch output to change each frame. This CCE design is created by enabling a convolutional encoder to alternate between two different generator matrices G_1 and G_2 using chaotic logistic map switch, as shown in Figure 1(b). The switching between g_1 and g_2 is implemented by adding a switch to one of the links of the adder. The position of the switch is controlled by the outputs of the one-dimension (1D) logistic map, which we design to work as a Chaotic Pseudorandom Binary Generator (CPRBG). By setting the threshold at (0.5) for each logistic map output (X_{n+1}), the switching output (γ) is binarized by setting $\gamma = 0$ if $X_{n+1} < 0.5$ and $\gamma = 1$ if $X_{n+1} > 0.5$. This binary output generates each frame, so the switching between polynomials g_1 and g_2 will change each turbo coding frame depending on the value of γ. As the output of this logistic CPRBG is 0 or 1, we use this binary output to switch between g_1 and g_2, respectively. The example shown in Figure 1(b) shows that, for CPRBG output 0, the switch is at g_1 and the generator matrix will be $G_1 = [1, 7/3]$ and if the CPRBG output is 1, then the switch is at g_2 and the generator matrix will be $G_2 = [1, 7/5]$. It means that the transmitted output changes each frame depending on the logistic CPRBG stream outputs.

The decoding process of the chaotic switching turbo decoder is slightly different from that of the conventional turbo decoder. Here, the decoder must switch between the trellises of the used different generators. Thus, for proper decoding, the decoder is required to have a copy of the secret key (initial parameters) to have the same CPRBG output sequence which increases the complexity of the decoder.

Consider the example shown in Figure 1(b) for the encoding process of a rate (1/2) systematic convolutional code; the switched generator matrix is $G_1 = [1, 7/3]$ and $G_2 = [1, 7/5]$ for each $\gamma = 1$ and $\gamma = 0$, respectively. The modified chaotic trellis diagram for a binary message $m = 1100$ with switching output $\gamma = 1001$ is shown in Figure 2. For each input binary

Table 1: Stream outputs for each state based on γ.

I/P m	States	O/P stream ($\gamma = 0$)		O/P stream ($\gamma = 1$)	
		u_1	$\mathbf{u_2}$	u_1	$\mathbf{u_2}$
0	00	0	**0**	0	**0**
1	00	1	**1**	1	**1**
0	10	0	**0**	0	**1**
1	10	1	**1**	1	**0**
0	01	0	**1**	0	**0**
1	01	1	**0**	1	**1**
0	11	0	**1**	0	**1**
1	11	1	**0**	1	**0**

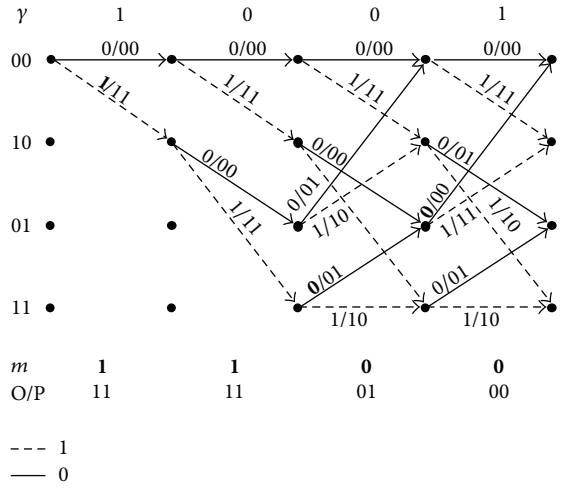

Figure 2: Modified chaotic trellis diagram.

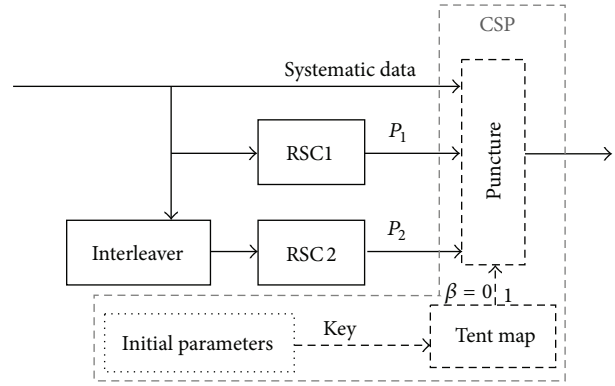

Figure 3: CPSTC design.

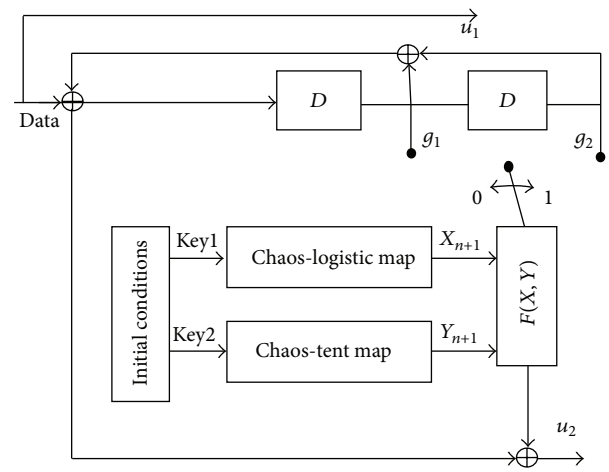

Figure 4: The CCCE encoder design.

message bit, the output $\mathbf{u_2}$ varies based on γ, as shown in Table 1.

For the chaotic switching decoder, each branch word output varies on the modified chaotic trellis branches according to the value of the switching parameter γ, as shown in Figure 2.

2.2. Chaotic-Switched Punctured Turbo Code. As we mentioned before, chaotic channel-coding schemes provide both data secrecy and data reliability in one process. The criteria for secured selection of component codes design chaotically using logistic CPRBG have been discussed in the previous CSTC scheme. The code rate is one of the effective parameters that affect the design of a concatenated turbo code. Therefore, for the second secured reliable scheme, the code rate varies depending on the binary stream output of 1D tent map which was used as a chaotic switch.

Figure 3 displays the second secure reliable turbo coding scheme which is CPSTC. On the architecture of the Chaos Switched Puncture (CSP) proposed in this scheme, the stream switching output of 1D tent CPRBG is fed to the turbo coder puncture.

This stream sequence works as a puncturing switch as with "0" there is no puncturing and the turbo coding rate $R_0 = 1/3$. However, for "1," the puncture is ON and the rate $R_1 = 1/2$. As in the CSTC, this switching process is each frame depending on the stream sequence output of the tent CPRBG. By setting the threshold at zero for each tent CPRBG output (Y_{n+1}), the switching output (β) of the chaos switch is binarized by setting $\beta = 0$ if $Y_{n+1} < 0$ and $\beta = 1$ if $Y_{n+1} > 0$.

The CPSTC rate will change each frame depending on β; if $\beta = 0$, then the puncture is off (no puncturing) and the code rate will be 1/3. If the chaos switch output $\beta = 1$, then the puncture is on (puncturing) and the code rate will be 1/2. As in CSTC, the CPSTC decoder is required to have a copy of the secret key (tent map initial parameters) to have the same CPRBG output sequence.

2.3. Coupled Chaotic-Switched Turbo Code. The Coupled Chaotic-Switched Turbo Code (CCSTC) encoder is created by enabling two coupled chaotic convolutional encoders (CCCE) to alternate between two connection polynomials g_1 and g_2 as shown in Figure 4. The construction of this system model is the same as CSTC in the encoder design, but it is different in the chaotic switching process as here we use coupled chaos switch that consists of two chaotic maps.

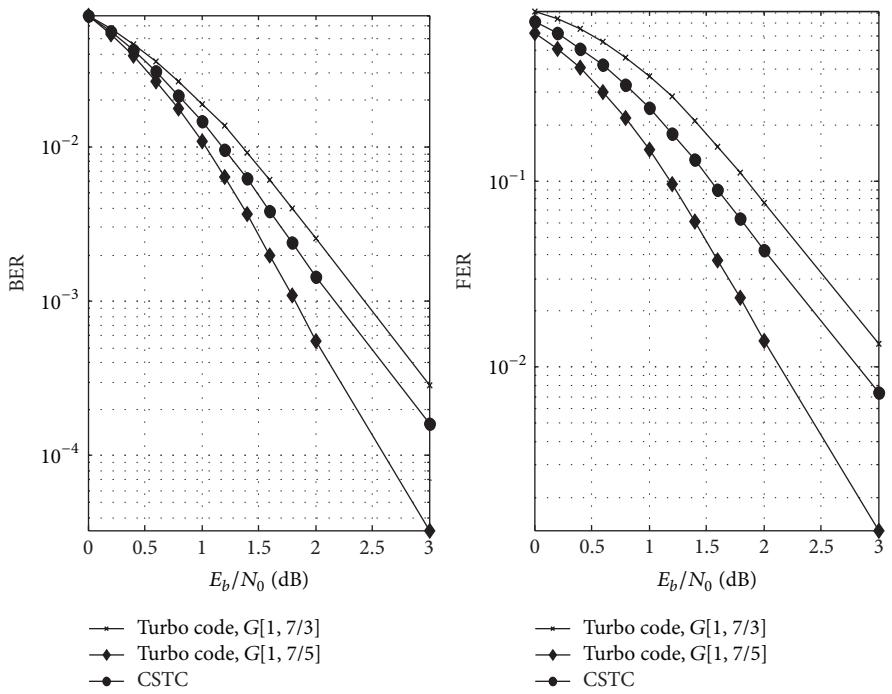

Figure 5: BER performance of CSTC with generator matrices $G_1 = [1, 7/3]$ and $G_2 = [1, 7/5]$.

In the previous two schemes, each CPRBG is based on single 1D chaotic map system and generates pseudorandom binary numbers directly from its orbit. In this scheme, we present another Coupled Chaotic Pseudorandom Binary Generator (CCPRBG) based on a couple of two chaotic maps, which can provide higher security than other previous schemes because two chaotic systems are employed to generate binary sequence. Since this sequence is generated by comparing two different chaotic orbits, it is difficult for an eavesdropper to extract information about both chaotic systems. In this proposed CCSTC, two different 1D logistic maps or 1D logistic and tent maps are employed and coupled together to generate binary output random sequences. As shown in Figure 4, random bit streams are generated by comparing the outputs of both the logistic and tent map X_{n+1} and Y_{n+1}, respectively, as

$$F(X,Y) = \begin{cases} 1 & \text{if } X_{n+1} > Y_{n+1} \\ 0 & \text{if } X_{n+1} \leq Y_{n+1}. \end{cases} \quad (1)$$

This binary sequence $F(X, Y)$ used as a switching element in the CSTC system model.

3. Simulation Analysis

3.1. BER Simulation Analysis. For the first simulated CSTC system, we have a transmitted frame size of $N = 128$ bits. The rate $R = 1/4$ turbo code uses random interleaver and two parallel CCE, with $g_1 = [7, 3]$ and $g_2 = [7, 5]$ as switched polynomials.

The turbo decoding algorithm used is the Log-MAP algorithm. Figure 5 depicts the BER and FER performances of the CSTC system in the Additive White Gaussian Noise (AWGN) channel, with zero-mean and variance $\sigma^2 = N_0/2$, where N_0 is the noise power spectral density. The performance of CSTC compared with two other classical turbo codes with fixed generator matrix design. As in our simulation the design of CSTC depends mainly on the switching between $G_1 = [1, 7/3]$ and $G_2 = [1, 7/5]$ generators, chaotic switching is not expected to give best performance of the codec but its performance is better than turbo system with $G_1 = [1, 7/3]$ (about 0.21 dB at BER 10^{-4} improvement) with incrementing the system security behavior. Figure 5 shows that the resulting BER performance of the designed CSTC is an average of the performances of the two conventional turbo configurations.

For the second simulated CPSTC system with the same simulated system parameters but with $G = [1, 7/5]$ and switched rates (1/2 or 1/3) turbo codes, Figure 6 compares the simulation performances between CPSTC and two other fixed rates conventional turbo code; the first is with code rate ($R_1 = 1/2$) and the other with ($R_2 = 1/3$). It is evident in Figure 6 that the resulting BER and FER performances of the designed CPSTC are an average of the performances compared with the other two conventional turbo configurations.

3.2. Chaotic Maps Simulation Analysis. Generally, the security of the above chaotic turbo coding systems can be ensured by the perfect secure properties of CPRBG. But we have known that many chaotic systems are not secure although they have some "good" statistical properties. So we should still investigate whether or not the ciphers based on digital CPRBG are secure enough to known cryptanalysis methods. As the unpredictability and the security of CSTC and CPSTC

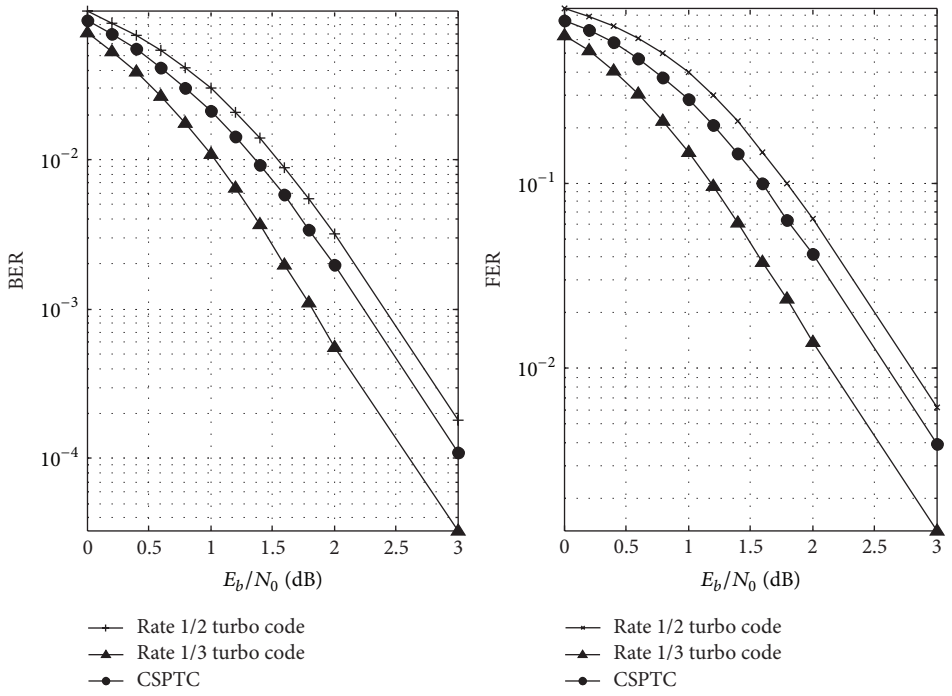

Figure 6: BER performance of CSPTC with $R_1 = 1/2$ and $R_2 = 1/3$.

systems principally depend on the logistic and tent CPRBG, it is rendering as the most critical and vital component of the system and it is very important to distinguish robustly whether a chaos CPRBG is chaotic or not. Many tests can be used for this aim, but the results of a much simpler "0-1" test for the presence of deterministic chaos in [26] show that this test is at least as robust as other methods for the detection of deterministic chaos in a noisy time series. This "0-1" test takes as input a time series of measurements and returns a single scalar value usually in the range [0, 1]. In the case of an infinite amount of noise-free data, the test result is near to "1" in the presence of deterministic chaos and zero otherwise.

3.2.1. Logistic Map. Because logistic map has been widely investigated in chaos theory and is very simple to be realized, it has been used by many digital chaotic applications.

The logistic map formula is

$$x_{n+1} = \mu x_n (1 - x_n), \quad 0 \le x_n \le 1, \quad 0 \le \mu \le 4, \tag{2}$$

where μ is the bifurcation parameter and x_n is the initial condition of the map. In this map, the next states x_{n+1} of the chaotic system are fully described only by its present state x_n. However, as shown in Figure 7, only when the bifurcation parameter (μ) falls in the region $3.57 < \mu \le 4$, the logistic map has perfect chaotic properties and the orbit diagram of the map reveals an unexpected mixture of order and chaos with periodic windows interspersed between chaotic clouds of dots.

For the logistic CPRBG orbits indicated in Figure 8(a) with bifurcation parameter ($\mu = 3.98$) and the initial condition ($x_n = 0.3$), the output of its "0-1" test is (0.9988) as shown in Figure 8(b).

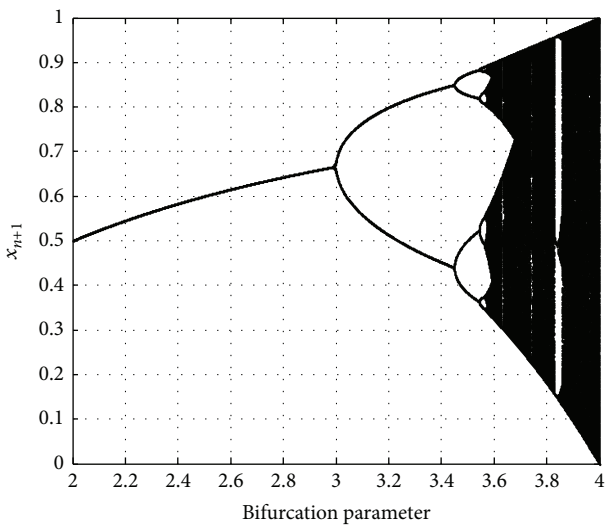

Figure 7: Logistic map bifurcation parameter (μ).

3.2.2. Tent Map. As the logistic map, tent map has been extensively studied due to its simplicity of hardware and software implementations. The form of tent map can be as follows:

$$y_{n+1} = \begin{cases} \mu y_n, & a \le y_n < \dfrac{1}{2} \\ \mu (1 - y_n) & \dfrac{1}{2} \le y_n \le b, \end{cases} \tag{3}$$

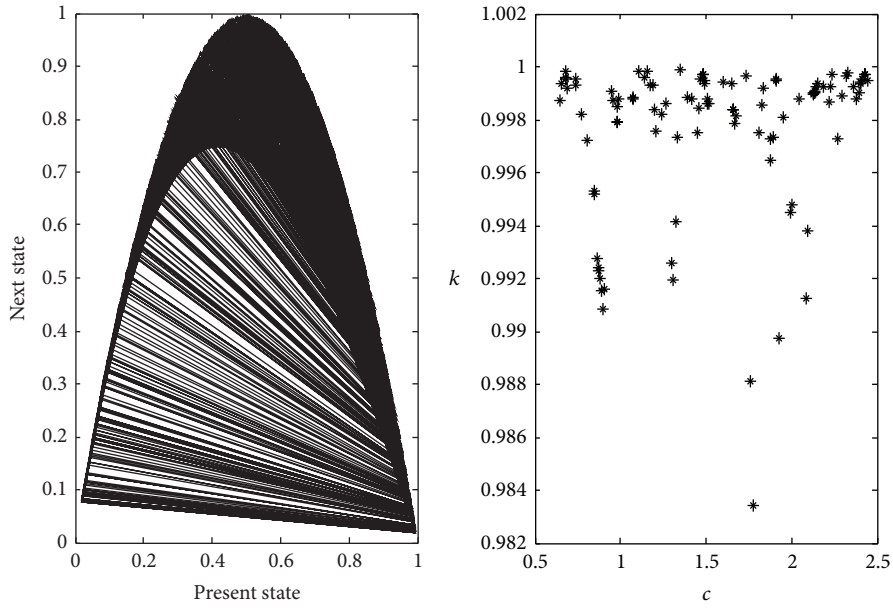

Figure 8: Logistic CPRBG (a) orbits of the logistic map and (b) "0-1" test result.

where b is a positive real constant $0 \leq b < 1$ and $y_n \in [0, 1]$. Equation (3) is an iterated function when $y_{n+1} = f_\mu(y_n)$, which generates orbits $\{y_0, y_1, y_2, y_3, \ldots\}$ that are sequences of real numbers defined at $[a, b] \in R$ with $a < b \in [0, 1]$. For certain parameter values, the mapping undergoes stretching and folding transformations and displays sensitivity to initial conditions and periodicity.

For our work we adjust the tent map as

$$y_{n+1} = A - (\mu y_n). \tag{4}$$

Figure 9(a) shows the graphical representation for the T-1D map orbits, which has two piecewise linear segments in the intervals, $[-0.5, 0]$ and $(0, 0.5]$.

Although the form of the tent map is simple and the equations involved are linear, for certain parameter values, this system can display highly complex behavior and even chaotic phenomena as shown in Figure 9(b) where this tent map succeeds in the "0-1" test with the test output equal to (0.997).

These results of both logistic and tent maps combine the chaotic behavior to the designed chaotic turbo codes with its error correction capabilities.

3.2.3. Coupled Chaotic Maps. The use of CCPRBG possesses excellent statistical and cryptographic properties. Normally when an intruder finds some information about the used chaotic map from their orbits, he might use such information to lessen the complexity of its preshared secret initial condition. With the use of coupled chaotic maps, the cryptanalysis of chaotic secrecy will be more difficult as the chaos output sequence depends on many different chaotic orbits.

As mentioned before, designing a CCPRBG provides higher security than other previous schemes because two different chaotic maps are employed to generate binary sequence. We can see the results of the 0-1 test based on CCPRBG in Figure 10 which indicates that it has a chaotic behavior with 0-1 test result equal to (0.998).

4. Chaotic-Switched Turbo Codes in Relay Channel

In the previous discussions, we focused on the point to point channel where a single transmitting and receiving node is used. In this section, we extend our proposed chaotic-switched turbo code to systems where three terminal nodes are used (relay channel). In this relay channel, we consider a half-duplex decode and forward relaying system. The system operates in a time-division manner. In the first time slot of the transmission, only the source sends a chaotic-switched coded packet representing N message bits. This transmission is received by both the relay and destination terminals.

After decoding and recoding, the relay node transmits its own codeword to the destination node in the second time slot. Therefore, the destination is considered to operate similarly to receiver selection diversity scenario. It receives two noisy observation sequences denoted by r_{SD} and r_{RD}, which are sent from source and relay, respectively. Different channels are considered, including the quasi-static flat-fading channel and the AWGN channel. We demonstrate that our proposed schemes applied consider the case that the source to relay link is perfect.

4.1. System Model. The relay system consists of three nodes: a source node (S), a relay node (R), and a destination node (D). This system has three directed transmission links: the links from source to destination, source to relay, and a relay

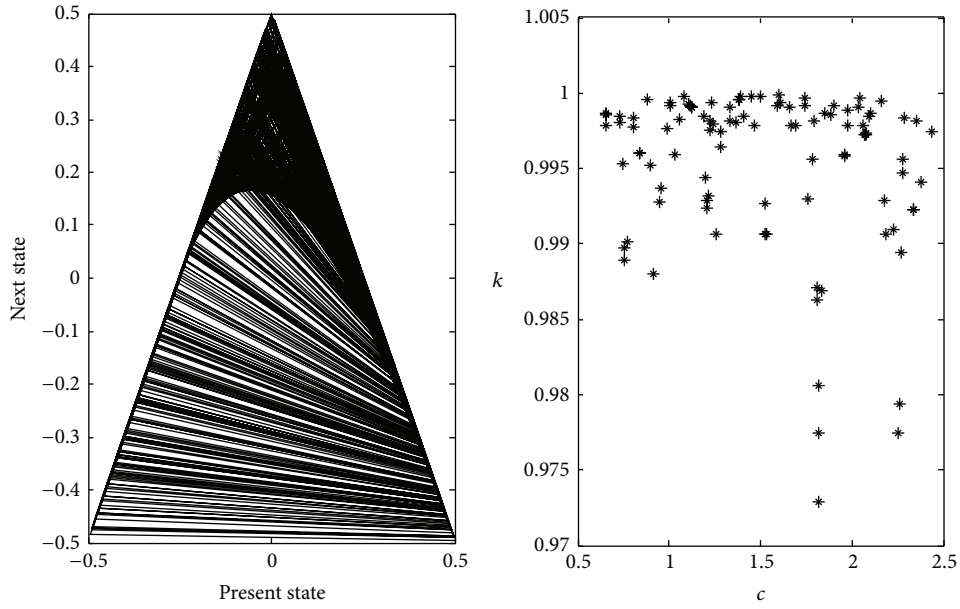

Figure 9: The tent CPRBG (a) tent orbits with $A = 0.5$, $\mu = 1.99$, and $y_n = 0.5$ and (b) "0-1" test result.

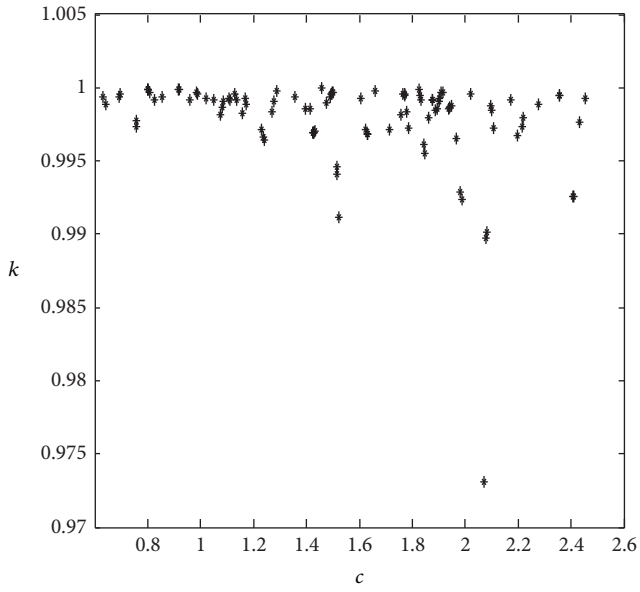

Figure 10: "0-1" test result of CCPRBG.

to destination link. We use AWGN and fast fading channels, and for fast fading channel we suppose that all the channel links are with independent fading on all three links, and their average SNRs are denoted by ξ, ξ_{SR}, and ξ_{RD}, respectively, with $\xi_{SR} = g_{SR}\xi$ and $\xi_{RD} = g_{RD}\xi$ where g_{SR} and g_{RD} are the source-relay and relay-destination channels gain, respectively. Typically, the source to relay and the relay to destination links have a larger SNR than the direct link; that is, $g_{SR} \geq 1$ and $g_{RD} \geq 1$, where the gains may be due to shorter transmitter/receiver separation. The overall SNR is defined by the SNR of the source to destination link, that is, by ξ.

Two steps are required to complete the transmission; during the first phase, the source broadcasts its information to both relay and destination. In the second phase, the relay processes the received data from the source by using decode and forward protocol and transmits the parity sequence generated from the processed data to destination while the source is in silent mode during this phase.

In the first time slot, the received signal z at the relay node is given by

$$z = \sqrt{g_{SR}} h_{SR} x_1 + n_1, \tag{5}$$

where x_1 is the symbol transmitted from the source with power P_0 during the first slot, n_1 is the AWGN term, and h_{SR} is the source-relay channel coefficient. When an AWGN channel is considered, $h_{SR} = 1$ and n_1 is a real Gaussian random variable with variance $N_0/2$. On the other hand, when a Rayleigh fading channel is considered, h_{SR} is a zero-mean complex Gaussian random variable with unit variance, and n_1 is also a zero-mean complex Gaussian random variable with variance of $N_0/2$ per dimension. The received signal at the destination from the relay node during the second time slots is given by

$$r_{RD} = \sqrt{g_{RD}} h_{RD} x_2 + n, \tag{6}$$

where x_2 is the symbol transmitted from the relay node with the power P_0. The source-destination and relay-destination channel coefficients are unity for an AWGN channel or zero-mean complex Gaussian fading coefficients with unit variance for a Rayleigh fading channel. The noise n has the same distribution as n_1. We consider the case that the source

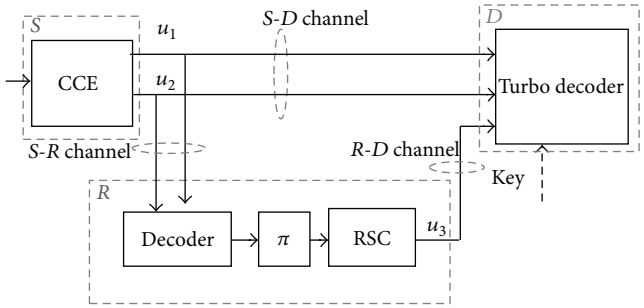

Figure 11: The design of DCSTC.

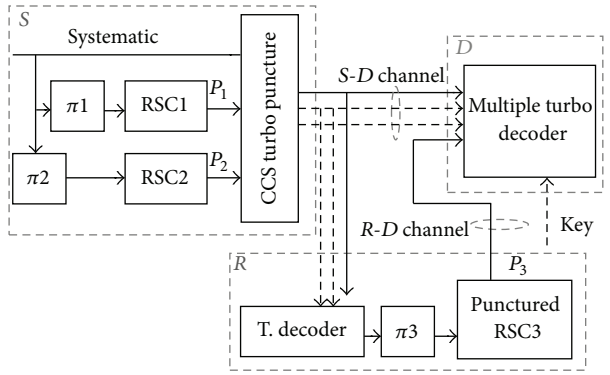

Figure 12: The design of CCPSTC.

to relay link is ideal; that is, $g_{SR} = \infty$. Also we assume that n, n_1, h_{SR}, h_{SD}, and h_{RD} are independent of each other, and they are assumed to be known perfectly at the receiver sides and unknown at the transmitter sides.

4.2. Extensions to Distributed Chaos Switched Turbo Codes (DCSTC). The major difference between distributed chaos switched coding and previous proposed chaos switched turbo coding schemes is that, in distributed coding, the overall codeword is constructed in a distributed manner. That is, different parts of the codeword in distributed coding are transmitted by different nodes through independent wireless links which creates additional degrees of freedom.

In a DCSTC system introduced in Figure 11, CCE and RSC encoders are used at the source node and the relay node, respectively. The source broadcasts the coded signals by the CCE to both the destination and relay. The relay decodes the received signals and interleaves and recodes them using punctured RSC. The destination receives two noisy observation sequences that consist of a coded signal at the source and the second parity transmitted from the relay.

4.3. Extensions to Cooperative Chaos Punctured Switched Turbo Code (CCPSTC). Here in this scheme turbo code is used at the source which consists of two simple constituent RSC1 and RSC2 encoders and Coupled Chaos Switched (CCS) puncture to alternate between two parity bits (P_1 and P_2). The source node transmits coded symbols to both the relay and the destination nodes during the first transmission period. The relay performs parallel concatenated codes decoding. It then recodes the information bits using a RSC3 code during the second transmission period. For each frame, the resultant symbols transmitted from the source and relay nodes can be viewed as the chaotic coded symbols of a three-component parallel concatenated encoder with overall rate alternated between (1/3) and (1/4) depending on the CCS binary stream output. Thus, at the destination, the chaotic-switched punctured turbo code is equipped with more parity bits. The destination decoder now receives two noisy, faded versions of the parallel concatenation of three recursive binary convolutional encoders with frame changed overall rate.

Figure 12 depicts the system diagram for the proposed CCPSTC system. Iterative decoding at the destination involves three MAP decoders, with extrinsic information exchange between modules in the manner of multiple turbo decoder [27] but here, for proper decoding, the decoder must know the CCS binary stream output (key or the initial conditions).

4.4. Simulation Results. In the previous section, we presented the designing of the proposed schemes for applying CSTC and CPSTC in the relay channel; here in this section we illustrate their performance via simulations and compare the results with the different switching rates systems. In our simulated DCSTC system, the source node transmits the CCE outputs (u_1 and u_2). After decoding, the relay node retransmits its parity bits (u_3) from the CRSC corresponding to the interleaved message bits.

Thus, at the destination, we can have an overall rate (1/3) turbo code. In each frame, the destination node applies 8-iteration maximum *a* posteriori (MAP) switched decoding depending on the used secret key (initial condition) after collecting the source transmitted bits in the first time slot and the extra parity bits transmitted from the relay node in the second time slot.

Figure 13 shows a comparison between the performance of noncooperative CSTC and the DCSTC in an AWGN channel with frame length = 128 bits, overall code rate equal to (1/3), and g_{RD} = 1 dB which implies a good performance of DCSTC due to the use of relay channel. As we mentioned before, chaotic switching turbo coding system is not expected to give best performance of the codec as it is a tradeoff between security and the system performance but for optimum secured reliable output of this system we use different switching rates. The performance of our proposed DCSTC is increasing as the switching rate is decreased. So we can control the system performance with the chaos switching rates as shown in Figure 13, where the BER of DCSTC at switching rate equal to 2, 5, and 10 (switching each 2, 5, and 10 frames) gives about 0.2, 0.5, and 0.6 dB gain, respectively (at 10^{-4} BER), compared to that with switching each frame which means that the BER and FER performances increased as the switching rate decreased.

Typical results are shown in Figure 14, plotting BER and FER versus E_b/N_0, of the proposed CCPSTC scheme in fast

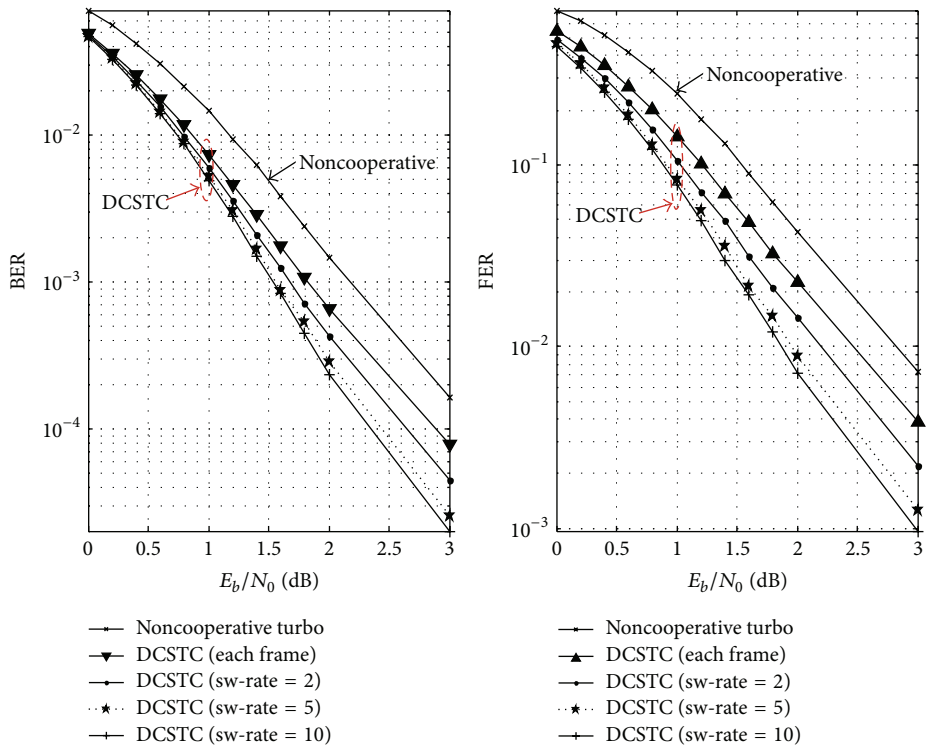

Figure 13: BER and FER comparison between no cooperative and distributed CSTC for different switching rates in AWGN channel and g_{RD} = 1 dB.

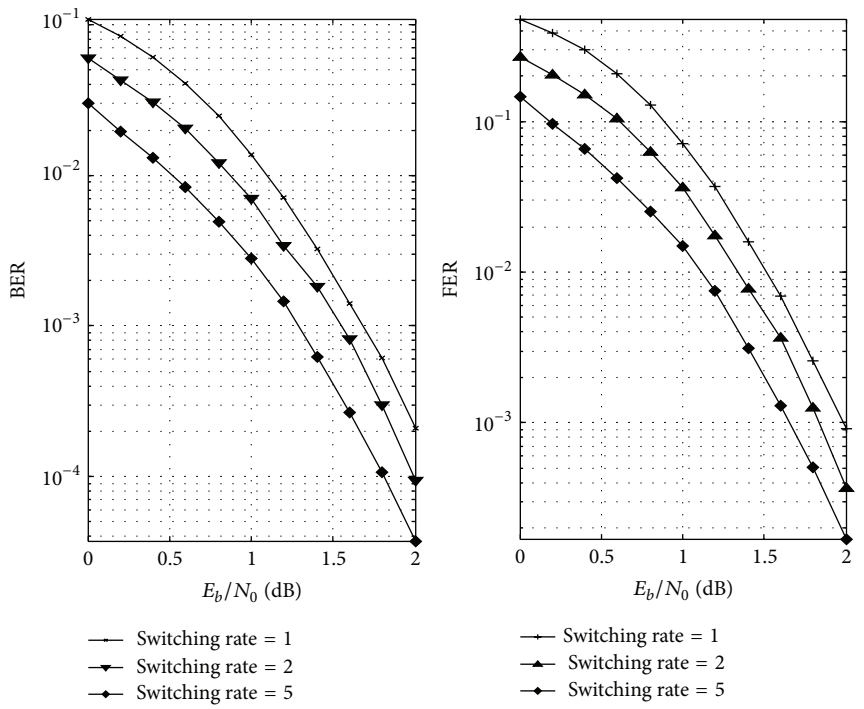

Figure 14: BER and FER of CCPSTC for different switching rates in fast fading and g_{RD} = 2 dB.

fading channel with $g_{RD} = 2\,\text{dB}$ and with frame switched overall code rate (1/3 and 1/4). Also, by controlling the switching rate of the used chaos switch, we can gain better secured reliable system performance.

5. Conclusion

In this paper, we have presented a combination of turbo coding design with chaotic dynamics. It is established that the proposed chaotic-switched turbo scheme is more secure than the conventional system, but with a slight error correction performance degradation especially for high switching rate. Two other chaotic switching cooperative turbo codes DCSTC and CCPSTC are also being proposed.

In these secured cooperative turbo coding schemes as we combine the secured reliable error correction codes with the diversity gain of the relay channel, a good error correction performance can be achieved. The analysis demonstrates that we can avoid the performance degradation due to the chaotic switching by reducing the chaotic switching rate which can give better BER and FER performances. This suggests that it is crucial to be mindful of the compromises between chaotic switching rate and error correction performance when adopting such heterogeneous scheme for channel-coding purposes.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by the Nanjing University of Aeronautics and Astronautics, Nanjing, China. The authors would like to thank the anonymous reviewers for their valuable suggestions and comments that helped to improve this work.

References

[1] R. Brown and L. O. Chua, "Clarifying chaos: examples and counterexamples," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 6, no. 2, pp. 219–249, 1996.

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[3] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, "From chaotic maps to encryption schemes," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '98)*, pp. 514–517, Monterey, Calif, USA, June 1998.

[4] G. Alvarez, G. P. F. Monotoya, G. Pastor, and M. Romera, "Chaotic cryptosystems," in *Proceedings of the IEEE 33rd Annual International Carnahan Conference on Security Technology*, pp. 332–338, Madrid, Spain, October 1999.

[5] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems. I. Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2001.

[6] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Physical Review Letters*, vol. 70, no. 20, pp. 3031–3034, 1993.

[7] X. Yongxiang, C. K. Tse, and F. C. M. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 51, no. 12, pp. 680–684, 2004.

[8] R. Bose and S. Pathak, "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," *IEEE Transactions on Circuits and Systems. I. Regular Papers*, vol. 53, no. 4, pp. 848–857, 2006.

[9] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[10] M. S. Baptista, "Cryptography with chaos," *Physics Letters A*, vol. 240, no. 1-2, pp. 50–54, 1998.

[11] R. Bose and A. Banerjee, "Implementing symmetric cryptography using chaos functions," in *Proceedings of the 7th International Conference on Advanced Computing and Communications (ADCOM '99)*, pp. 318–321, December 1999.

[12] E. Alvarez, A. Fernández, P. Garcí, J. Jiménez, and A. Marcano, "New approach to chaotic encryption," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 263, no. 4-6, pp. 373–375, 1999.

[13] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems. I. Fundamental Theory and Applications*, vol. 48, no. 2, pp. 163–169, 2001.

[14] L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm," *Physics Letters A*, vol. 289, no. 4-5, pp. 199–206, 2001.

[15] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, pp. 238–242, 2002.

[16] S. Li, X. Zheng, X. Mou, and Y. Cai, "Chaotic encryption scheme for real-time digital video," in *Real-Time Imaging VI*, vol. 4666 of *Proceedings of SPIE*, pp. 149–160, January 2002.

[17] S. Kozic and M. Hasler, "Low-density codes based on chaotic systems for simple encoding," *IEEE Transactions on Circuits and Systems. I. Regular Papers*, vol. 56, no. 2, pp. 405–415, 2009.

[18] T. Y. Ng, L. Y. Chew, and S. Puthusserypady, "Error correction with chaotic switching between convolutional codecs," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 55, no. 11, pp. 3655–3662, 2008.

[19] F. J. Escribano, S. Kozic, L. López, M. A. F. Sanjuán, and M. Hasler, "Turbo-like structures for chaos encoding and decoding," *IEEE Transactions on Communications*, vol. 57, no. 3, pp. 597–601, 2009.

[20] F. J. Escribano, A. Wagemakers, and M. A. F. Sanjuan, "Chaos-based turbo systems in fading channels," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 2, pp. 530–541, 2014.

[21] F. J. Escribano and A. Tarable, "Interleaver design for parallel concatenated chaos-based coded modulations," *IEEE Communications Letters*, vol. 17, no. 5, pp. 834–837, 2013.

[22] W. K. Harrison, J. Almeida, S. W. McLaughlin, and J. Barros, "Coding for cryptographic security enhancement using stopping sets," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 575–584, 2011.

[23] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, 2012.

[24] N. Živić and M. F. Flanagan, "On joint cryptographic verification and channel decoding via the maximum likelihood criterion," *IEEE Communications Letters*, vol. 16, no. 5, pp. 717–719, 2012.

[25] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and encoding: turbo-codes," in *Proceedings of the IEEE International Conference on Communications*, pp. 1064–1070, Geneve, Switzerland, May 1993.

[26] G. A. Gottwald and I. Melbourne, "On the implementation of the 0-1 test for chaos," *SIAM Journal on Applied Dynamical Systems*, vol. 8, no. 1, pp. 129–145, 2009.

[27] D. Divsalar and F. Pollara, "Multiple turbo codes," in *PRoceedings of the IEEE Military Communications Conference (MILCOM '95)*, vol. 1, pp. 279–285, San Diego, Calif, USA, November 1995.