Turbo-Like Structures for Chaos Encoding and Decoding

Francisco J. Escribano, *Member, IEEE*, Slobodan Kozic, Luis López, Miguel A. F. Sanjuán,
and Martin Hasler, *Fellow, IEEE*

***Abstract*—In this paper, we explain how to build a turbo-like structure with binary inputs and chaotic outputs for efficient coding and decoding in additive white Gaussian noise (AWGN). We analyze the convergence of the decoding algorithm, the performance in the error floor region and explain minimum distance properties of the resulting codes.**

***Index Terms*—Channel coding, chaos, concatenated coding, modulation coding, error analysis.**

I. Introduction

THE possibility of using chaotic signals to carry information was first proposed in 1993 [1]. The interest in chaotic communications was related to the supposed good properties of the signals produced by chaotic systems from the point of view of secure or broadband multiple access systems, but they were not so successful as encoding or modulation systems. However, the proposal of chaos based coded modulations [2], which allow a convolutional coder point of view, opened a road to evaluate such kind of encoders when introduced in very efficient concatenated encoding systems, as is the case with parallel concatenation of channel codes [3]. It can be expected that new systems built under the same principles would lead to comparable results. Another advantage of designing systems under the similarities brought up by these new proposals is that we can use well established tools borrowed from communication theory, and apply them to chaos based systems without the need of an approach based on complex chaos theory. As a consequence, we address here the design of parallel concatenated encoding and decoding systems including two chaotic encoders with real-valued outputs linked by means of a binary interleaver. We will show that we can get results comparable to standard binary turbocodes, and that conventional analysis tools adapted to this new framework can give valuable insight into the main features of these promising parallel concatenated systems.

II. System Description

The concatenated encoder consists of two rate 1 chaotic-like encoders fed with a binary input $\{b_n\}$ and its interleaved image $\{c_n\}$ [3]. The interleaving is performed with permutations over bit blocks of size N, $\mathbf{b} = \{b_1, b_2, \cdots, b_N\}$, and produces an interleaved word $\mathbf{c} = \{c_1, c_2, \cdots, c_N\}$. The outputs $\mathbf{x} = \{x_1, x_2, \cdots, x_{2N}\}$ are codewords of size $2N$, which are formed by taking alternatively values from both encoders. The resulting rate is $R = 1/2$. The main difference with respect to the previous state of art in turbocodes is the presence of chaotic systems as encoders on each branch. These chaotic encoders are in fact chaotic maps controlled by small perturbations as presented in [2]. They are described by a recursion in the form

$$z_n = f\left(z_{n-1}, b_n\right) + g\left(z_{n-1}, b_n\right) 2^{-(Q+1)}, \tag{1}$$

where both applications $f(\cdot, 0)$ and $f(\cdot, 1)$ leave the interval $[0, 1]$ invariant. In addition, they are piecewise linear with slope ± 2 wherever it is defined. The natural number $Q+1$ indicates the number of bits to represent z_n. $g\left(z_{n-1}, b_n\right)$ is the binary function $g\left(z_{n-1}, b_n\right) = b_n$ if $z_{n-1} < 1/2$, and $g\left(z_{n-1}, b_n\right) = \overline{b}_n$ if $z_{n-1} > 1/2$. This function is responsible for the small perturbation of the chaotic sequence, and is equivalent to a recursive precoder needed for any outer encoder in a parallel concatenated scheme in order to get interleaver gain [3]. The recursion (1) leaves a finite set invariant, and therefore we can restrict it to $S_Q = \{m \cdot 2^{Q+1} - 1 | m = 0, 1, \cdots, 2^{-(Q+1)}\}$. When $Q \rightarrow \infty$, equation (1) becomes simply the recursion by the chaotic maps $f(\cdot, 0)$ and $f(\cdot, 1)$, depending on the value of b_n (c_n for the second chaotic encoder). The chaotic samples z_n are normalized to $[-1, 1]$ as $x_n = 2z_n - 1$ before sending them to the channel. Note that these chaotic encoders are intrinsically non-systematic.

In this paper, we will consider different pairs of applications $f(\cdot, 0)$ and $f(\cdot, 1)$:

1) Tent map (TM):

$$f(z, 0) = f(z, 1) = 1 - |2z - 1|. \tag{2}$$

2) A shifted and replicated version of Bernoulli shift map, which we will call multi-BSM (mBSM):

$$\begin{aligned} f(z, 0) &= 2z \mod 1, \\ f(z, 1) &= 2z + 1/2 \mod 1. \end{aligned} \tag{3}$$

Paper approved by K. Narayanan, the Editor for Coding and Communication Theory of the IEEE Communications Society. Manuscript received September 15, 2006; revised May 8, 2008 and July 4, 2008.

We acknowledge financial support from the Spanish Ministry of Education and Science under Project FIS2006-08525, from the Spanish Ministry of Science and Technology under Grant TSI2006-07799, from the Comunidad de Madrid under Grant S-0505/TIC/0285, from the Research Program of the Universidad Rey Juan Carlos under Project URJC-CM-2007-CET-1601, and from the Swiss National Science Foundation under Project 200020-109474.

F. J. Escribano is with the Department of Signal Theory and Communications, Universidad Alcalá de Henares, 28805 Alcalá de Henares, Spain (e-mail: francisco.escribano@ieee.org).

S. Kozic was with the School of Computer and Communication Sciences (I&C), EPFL, CH-1015 Lausanne. He is now with Current Technologies International, CH-5506 Maegenwil, Switzerland (e-mail: slobodan.kozic@epfl.ch).

M. A. F. Sanjuán is with the Departamento de Física and L. López is with the Departamento de Sistemas Telemáticos y Computación, Universidad Rey Juan Carlos, 28933 Móstoles, Spain (e-mail: {miguel.sanjuan, luis.lopez}@urjc.es).

M. Hasler is with the I&C, EPFL,CH-1015 Lausanne, Switzerland (e-mail: martin.hasler@epfl.ch).

Digital Object Identifier 10.1109/TCOMM.2009.03.060520

3) Multi-tent map (mTM):

$$\begin{aligned} f(z,0) &= 1-|2z-1|, \\ f(z,1) &= 3/2-|2z-1| \mod 1. \end{aligned} \tag{4}$$

The systems described by (1) can be represented by means of a recursive convolutional encoder and a mapping to the signal constellation given by S_Q. Thus, the system is in fact equivalent to a trellis coded modulation (TCM) [3], and we will call it a chaos coded modulation system [2]. Therefore, the turboencoder system derived from the concatenation of these chaotic encoders will be very similar to a turbo-TCM system. The equivalent finite-state recursive convolutional encoder is given by

$$\begin{aligned} v_{Q+1}^{n} &= u_1 v_{Q+1}^{n-1} \oplus u_2 v_{Q}^{n-1} \oplus u_3 b_n, \\ v_{i}^{n} &= u_4 v_{i-1}^{n-1} \oplus u_5 v_{Q+1}^{n-1}, \qquad i = Q, \cdots, 2, \\ v_{1}^{n} &= u_6 v_{Q+1}^{n-1} \oplus u_7 b_n. \end{aligned} \tag{5}$$

where v_i^n are contents of the memory positions i at time n, and $u = (u_1, u_2, \cdots, u_7)$ is a binary vector. The mapping to the signal constellation is given by $z_n = \sum_{i=1}^{Q+1} 2^{-(Q+2-i)} v_i$. For $u = [1,1,0,1,1,1,1]$, $u = [1,1,1,1,1,1,1]$ and $u = [0,1,1,1,0,1,1]$, the system is equivalent to TM, mTM and mBSM respectively.

Based on the same principles, we can consider inverse chaotic dynamics for the chaos coded modulated codewords, instead of forward dynamics. A form of inverse dynamics with a multi-tent map (ImTM) is given by:

$$z_n = f_{BSM}^{Q}(z_{n-1}) + \left(1 - 4\left(f_{BSM}^{Q}(z_{n-1})\right)\right)\frac{z_{n-1}}{2} + \\ + \frac{g(z_{n-1}, b_n)}{2}, \tag{6}$$

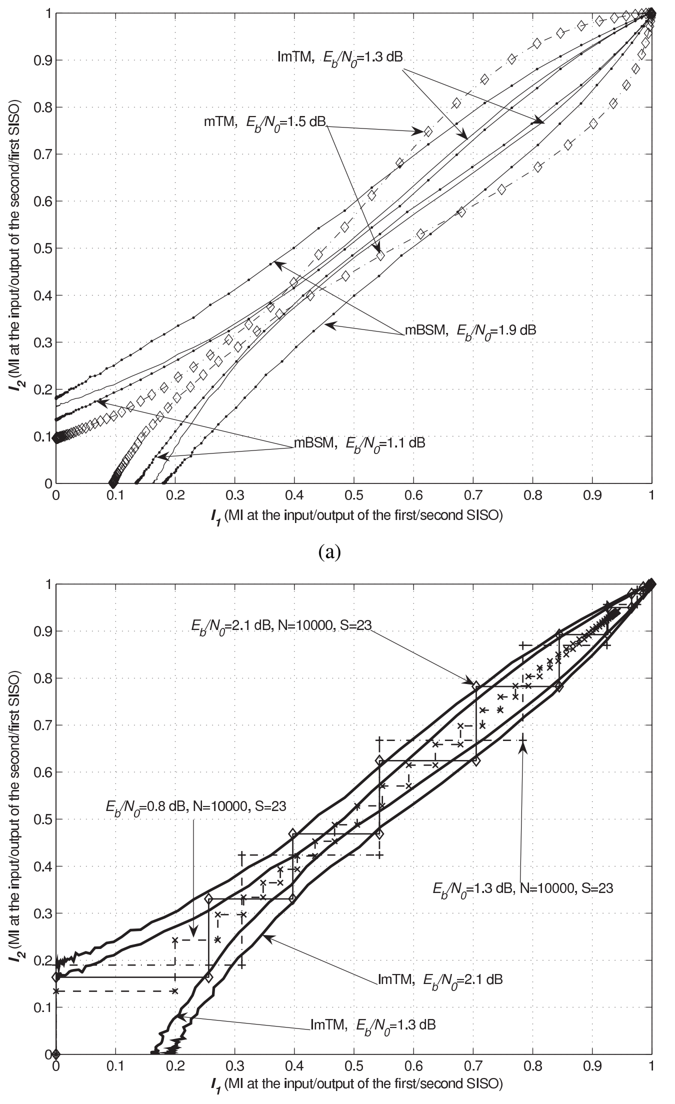
where $f_{BSM}^{Q}(z_{n-1})$ is the Q-th iteration of the Bernoulli shift map, $f_{BSM}(z_n) = 2z_{n-1} \mod 1$. For this system, $u = [1,1,0,1,1,1,1]$ and the signal constellation is $z_n = \sum_{i=1}^{Q+1} 2^{-i} v_i$.

The interleaver used in our examples will be either an S-random interleaver, with a minimum output separation of S positions between contiguous input bits, or a standard Cdma2000 interleaver [3]. With respect to the decoder, it will be an iterative decoding system based on soft-input soft-output (SISO) modules [3], but adapted to the chaos based coded modulations. These SISO modules accept as input the distorted values from the channel and a set of *a priori* binary log-likelihood ratios (LLR's), and give as output the corresponding *a posteriori* binary LLR's. These modules are based on the known log-MAP decoding algorithm for binary turbocodes, but with the needed arrangements for chaos coded output symbols [4]. The complexity of the MAP algorithm is proportional to 2^Q.

III. Convergence Analysis

In this Section we will explore the turbo-like chaotic system by analyzing the iterative decoding algorithm. A powerful tool to perform this task is the so called Extrinsic Information Transfer (EXIT) chart [3]. The EXIT charts are based on the computation of the mutual information (MI) of the LLR's at the output of each SISO module, as a function of the MI of the input LLR's. The MI is normalized between 0 and 1, and, the closer the MI to 1, the higher the probability to decode without error [3]. For a particular signal to noise ration (E_b/N_0) in the channel, each of the SISO decoders will be characterized by an MI plot, as seen in Fig. 1(a). If the MI plots for both SISO intersect in one point before $(1,1)$, then the decoding algorithm does not fully converge, the MI interchange on iterative decoding gets stuck on this fixed point, and the resulting bit error rate (BER) is high. As E_b/N_0 grows, the MI move progressively apart, and finally a clearance between both MI plots appears. Thus, we have reached the waterfall region, where the MI interchange can proceed to the $(1,1)$ point and the BER usually drops dramatically. From this threshold E_b/N_0 value and on, we will be in the error floor region, where the BER of the turbo system often goes down smoothly again.

We have computed the EXIT charts as functions of E_b/N_0 for the SISO decoders associated to the coded modulation



(a)

(b)

Fig. 1. (a) EXIT charts for different turbo-like chaos based encoding systems with $Q = 4$ as a function of channel noise Upper curve: first SISO. Lower curve: second SISO. (b) EXIT chart and average trajectory of MI for the ImTM system with $Q = 4$.

systems, so that we can give an estimation of the location of the waterfall region. In Fig. 1(a) we have depicted several examples for $Q = 4$. According to them, we can predict that the sudden BER slope descent will be located around 1.3 dB for the ImTM system, around 1.1 dB for mBSM, around 1.5 dB for mTM, and around 2.7 dB for TM (not depicted). Note how the plots separate as E_b/N_0 grows (mBSM for 1.9 dB). Though not shown, the results for other values of the quantization parameter ($Q = 3, 5, 6$) practically coincide. This means that the convergence in decoding is mainly linked to the underlying chaotic system, and not to the finite-state machine implementation. The invariance with respect to Q is a desired property in this kind of systems, because it means we can use in practice a system with Q as low as possible (and thus with limited complexity), while being able to analyze it as a chaotic system with $Q \to \infty$.

These predictions will be validated by simulation. We will see though that the threshold E_b/N_0 values are located a bit before the predicted ones. In Fig. 1(b), we have depicted, together with the theoretical EXIT charts for the concatenation of two ImTM encoders, some examples of the average MI trajectory on iterative decoding with an S-random interleaver with $N = 10000$ and $S = 23$. We see that there is a progressive mismatch between average values and theoretical plots, mainly in the central zone where the bottleneck between MI plots usually takes place. As a consequence, convergence will happen a few tenths of dB earlier, near 0.8 dB for ImTM (see Fig. 1(b)). The disagreement appears because the EXIT charts have been built under the assumption of Gaussian distributed LLR's (which is not exactly true) and under the assumption of independent LLR's between SISO modules (which only becomes true for infinite size interleavers) [3].

IV. Minimum Distance Analysis

In parallel concatenation, the minimum distance of the resulting parallel concatenated code or coded modulation is usually employed to provide a bound on the error floor region [3]. An accurate description of the BER at the error floor region is a very important issue, since it gives an estimation of the code behavior in a zone often difficult to reach by simulation. The chaos based coded modulations described here are not linear, and they do not comply in general with the uniform error property [5]. Therefore, the analysis in search of minimum distance codewords could result in unfeasible calculations. However, we will see that, with the help of the interleaver structure, the task to find the minimum distance can be addressed. Let us define the simple binary input error event $\mathbf{e} = \mathbf{b} \oplus \mathbf{b}'$, where $\mathbf{e}$ has $w(\mathbf{e})$ nonzero bits that produce an error loop of length L. This error event, in association with all possible input words $\mathbf{b}$, induces a set of possible output squared Euclidean distances between the resulting codewords $\mathbf{x}$ and $\mathbf{x}'$ (associated to input words $\mathbf{b}$ and $\mathbf{b}'$ respectively), defined as $d_E^2 = d^2(\mathbf{x}, \mathbf{x}') = \sum_{n=m}^{m+L-2}(x_n - x'_n)^2$. The corresponding error loop in $\mathbf{x}$ and $\mathbf{x}'$ has length $L - 1$. Note that this distance depends on $\mathbf{e}$ and $\mathbf{b}$, and not only on $\mathbf{e}$ as in linear codes. In general, this value will also depend on Q, though the dependence is small [2].

Each chaos based coded modulation of the kind described has a characteristic binary error event which, in combination with a particular value of input word $\mathbf{b}$, leads to the absolute minimum output squared Euclidean distance of the chaos coded modulation [2]. However, in parallel concatenation with linear codes and interleavers, we are normally interested in weight 2 binary error events as major candidates for minimum distance [3]. In fact, due to the presence of the mentioned recursive precoding to ensure the interleaver gain, all the described chaos based coded modulations allow an input binary error event of minimum weight $w(\mathbf{e}) = 2$ and length $L^o = Q + a$ ($a = 2$ for mBSM, and $a = 3$ for TM, ImTM and mTM) which leads to low output squared Euclidean distances[1]. Let us denote the minimum squared Euclidean distance associated to these events as $d^2_{L^o,\min}$. Binary error events of length $L = p(L^o - 1) + 1$, $p \in \mathbb{N}$, are also possible, but the associated output squared Euclidean distances will be basically the same as with the minimal loop L^o, but scaled by p. Though $d^2_{L^o,\min}$ depends on $\mathbf{b}$, due to the finite memory of the equivalent finite-state encoding machine, there are only 2^{Q+L_0} possibilities to evaluate (2^{Q+1} possible values for the starting state, and 2^{L_0-1} possible input bits in $\mathbf{b}$ till the states merge again).

Therefore, if the interleaver takes two bits separated in $\mathbf{b}$ by L_1^o positions and maps them at the output as two bits separated by L_2^o positions[2], the minimum distance can be easily given as the sum of the minimum distances for each chaos coded modulation, $d^2_{E,\min} = d^2_{L_1^o,\min} + d^2_{L_2^o,\min}$. If the interleaver structure is such that two input bits separated by L_1^o positions are mapped at least $3L_2^o$ positions apart at the output, the most probable $\mathbf{e}$ will have weight 4 and will consist in the concatenation of two error events in $\mathbf{b}$ of the L_1^o kind that lead in $\mathbf{c}$ to other two error events of the L_2^o kind (provided that the interleaver allows this concatenation of error events). In this case, the minimum squared Euclidean distance will be $d^2_{E,\min} = 2d^2_{L_1^o,\min} + 2d^2_{L_2^o,\min}$. If the interleaver is built in such a way that two input bits separated by L_1^o positions are always mapped at least $2L_2^o$ positions apart, but not necessarily more than $3L_2^o$, the candidate minimum squared Euclidean distance will be like $d^2_{E,\min} = d^2_{L_1^o,\min} + 2d^2_{L_2^o,\min}$ for $\mathbf{e}$ with $w(\mathbf{e}) = 2$. For example, for ImTM with $Q = 4$, $L^o = 7$ and $d^2_{L^o,\min} \approx 1.335938$, so that, if we have an S-random interleaver with $S > 3L^o = 21$, the dominant $\mathbf{e}$ will consist on the mentioned composition of two weight 2 binary error events, and the parallel concatenation of two ImTM modules will have $d^2_{E,\min} = 4d^2_{L^o,\min} \approx 5.343752$. For mBSM with $Q = 5$, $L^o = 7$ and $d^2_{L^o,\min} \approx 1.271484$, so that, in the same situation, $d^2_{E,\min} = 4d^2_{L^o,\min} \approx 5.085936$.

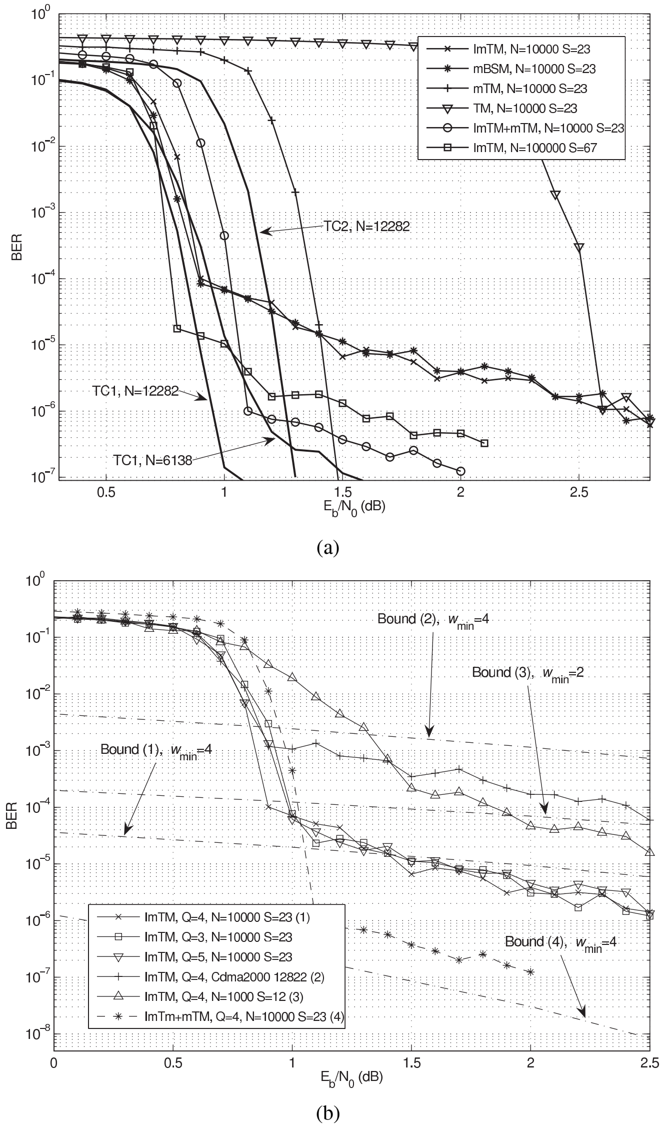
Once we have the minimum squared Euclidean distance, the bound for the error floor can be given as [3]

$$P_{b_{\text{floor}}} \approx \frac{w_{\min} N_{\min}}{2N} \operatorname{erfc}\left(\sqrt{\frac{d^2_{E,\min}}{4P} R \frac{E_b}{N_0}}\right), \qquad (7)$$

where $w_{\min}$ is 2 of 4 depending on the kind of binary error event under consideration, $N_{\min}$ is the number of possible

[1] These error events are not necessarily those leading to the absolute $d^2_{E,\min}$ for each chaos coded modulation. But they are normally the most probable ones in concatenation, since the events with $w(\mathbf{e}) > 2$ are usually prevented to happen in both encoders due to the interleaving.

[2] L_i^o, $i = 1, 2$, is the $w(\mathbf{e}) = 2$ minimal error event loop length for the first and second chaos coded modulations, respectively.



(a)

(b)

Fig. 2. (a) BER of systems TC1 and TC2 with Cdma2000 interleavers with $N = 6138$ and $N = 12282$, compared with several turbo-like chaotic systems with S-random interleavers and $Q = 4$ in all the cases. (b) BER and bounds for several turbo-like chaotic systems.

mappings $L_1^o \rightarrow L_2^o$, $L_1^o \rightarrow 2L_2^o$ ($w_{\min} = 2$), or $L_1^o, L_1^o \rightarrow L_2^o, L_2^o$ ($w_{\min} = 4$) allowed by the interleaver structure, $P \approx 1/3$ is the average power of the chaos coded modulated sequence[3], and $R = 1/2$ is the code rate. Note that this bound will be somewhat conservative, since (7) assumes that all the error events in the error floor region correspond to the predicted $d^2_{E,\min}$. This will not be in general true due to the nonlinear structure of the chaos coded modulations. However, it can still give valuable insight into the asymptotic behavior of the error floor.

V. Simulation Results

We have included for comparison the results for two rate $1/2$ binary turbocodes. The first one (TC1) is the rate $1/2$ punctured turbocode of Cdma2000 standard consisting on two rate $1/2$ and memory 3 recursive and systematic convolutional (RSC) encoders [3]. The second one (TC2) is also a rate $1/2$ punctured turbocode containing two rate $1/2$ and memory 4 RSC encoders with generator polynomials 33 (feedback) and 31 (feedforward) [3]. In Fig. 2(a), we compare these TC1, TC2 systems and the resulting turbo-like chaotic systems. The results are for 20 decoding iterations. The complexity is proportional to 2^3 for TC1, to 2^4 for TC2 and to 2^4 for the chaos based systems. Systems combining 2 ImTM or 2 mBSM blocks with $N = 10000$ S-random interleavers with $S > 3L^o$ have waterfall regions near the predicted thresholds, even improving the results of TC1 and TC2. As a tradeoff, the error floor is very high. The exception is the ImTM case with $N = 100000$, where the error floor decreases with $1/N$ as expected for this kind of concatenation [3]. Note that the slope in the error floor is the same, indicating that the minimum distance is really the same as with $N = 10000$. The concatenation of 2 mTM or 2 TM blocks lead to low error floors ($< 10^{-8}$ for mTM), but their waterfall thresholds are above the zone of interest, where TC1 and TC2 are located. Note how the inverse dynamics of ImTM improves the waterfall threshold of mTM, but provides a worse error floor. One way of overcoming this lies in combining two systems, for example an ImTM encoder with good convergence threshold and an mTM encoder with extremely low error floor. The result confirms that, in fact, we can still get a system with waterfall region near $E_b/N_0 = 1.0$ dB, and an error floor below 10^{-6}. Therefore, for similar complexity, we can get results comparable to binary turbocodes, though turbo TCM schemes will slightly outperform these chaos based schemes [3]. Note also how the error floors of TC1 and TC2 are almost always lower than the rest of cases, making it clear that the minimum distances of TC1 and TC2 are higher, with exception of the mTM system (TC2 and mTM have both error floors below 10^{-9}).

In Fig. 2(b), we compare the results with different interleavers and different Q and S factors. We verify how the influence of Q is small, affecting a little the E_b/N_0 threshold for the waterfall region and keeping the same error floor. As $S = 23 > 3L^o$, we have provided the bound with $w_{\min} = 4$ and, though not very tight, it is still accurate enough. The case with the Cdma2000 $N = 12822$ interleaver is much worse since the multiplicity of the $w_{\min} = 4$ errors goes from $N_{\min} = 4$ for the S-random interleaver to $N_{\min} = 491$ for this kind of interleaver designed with a rich structure intended for the Cdma2000 convolutional code. The ImTM results for the $N = 1000$, $S = 12 < 3L^o$ S-random interleaver fit well with the expected behavior of a poorer minimum distance (like $3d^2_{L^o,\min}$) and a higher multiplicity of the related $w_{\min} = 2$ errors ($N_{\min} = 45$). Finally, we can also see the bound for the ImTM+mTM case. Now the error floor is not upper bounded as in the rest of cases, meaning that there will be other important error events apart form the mentioned $w_{\min} = 4$ ones, though the BER slope yields still a good approximation.

VI. Conclusions

In this paper, we have proposed a turbo-like framework containing chaos based coding and decoding systems. We have shown that the performance can be comparable with

[3] This is only exact for $Q \rightarrow \infty$ [2]. For $Q \geq 4$, the difference can be considered negligible.

standard turbocodes and that, with the help of adapted known tools, we can locate the waterfall region and the error floor region in the BER plots with enough accuracy. We have also seen that the nonlinearity of these systems, together with a good combination of different chaotic modulations, may help to improve the final result. This is made possible because these systems push further the principle for turbocodes that their success lies in combating multiplicities rather than just increasing minimum distance [3]. All this makes this kind of turbo-like chaotic systems of potential interest in digital communications.

References

[1] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, no. 20, pp. 3031–3034, May 1993.

[2] S. Kozic, T. Schimming, and M. Hasler, "Controlled one- and multi-dimensional modulations using chaotic maps," *IEEE Trans. Circuits Syst. I*, vol. 53, pp. 2048–2059, Sept. 2006.

[3] C. B. Schlegel and L. C. Pérez, *Trellis and Turbo Coding*. New York: John Wiley & Sons, Inc., 2004.

[4] F. J. Escribano, L. López, and M. A. F. Sanjuán, "Iteratively decoding chaos encoded binary signals," in *Proc. Eighth IEEE International Symposium on Signal Processing and Its Applications (ISSPA) 2005*, vol. 1, Sydney, Australia, Aug. 2005, pp. 275–278.

[5] E. Biglieri and P. J. McLane, "Uniform distance and error properties of TCM schemes," *IEEE Trans. Commun.*, vol. 39, no. 1, pp. 41–53, Jan. 1991.