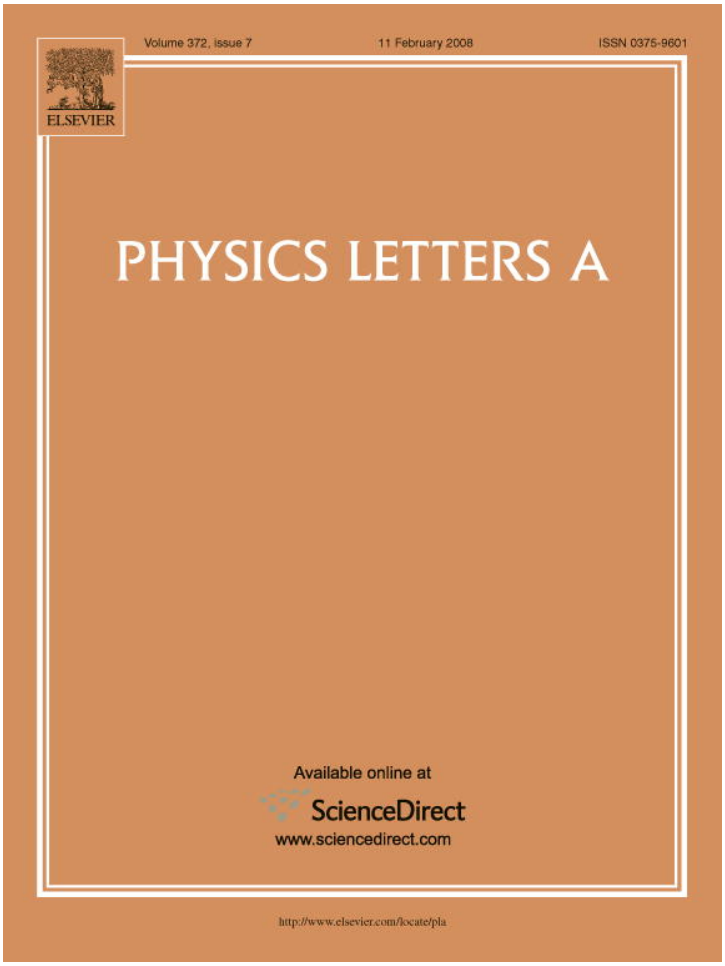

Available online at www.sciencedirect.com
ScienceDirect
Physics Letters A 372 (2008) 1018–1023
PHYSICS LETTERS A
www.elsevier.com/locate/pla

Encryption test of pseudo-aleatory messages embedded on chaotic laser signals: An information theory approach

O.A. Rosso [a,b,*], R. Vicente [c,d], C.R. Mirasso [e]

[a] *Centre for Bioinformatics, Biomarker Discovery and Information-Based Medicine, School of Electrical Engineering and Computer Science, The University of Newcastle, University Drive, Callaghan NSW 2308, Australia*
[b] *Chaos & Biology Group, Instituto de Cálculo, Facultad de Ciencias Exactas y Naturales, Pabellón II, Ciudad Universitaria, 1428 Ciudad Autonoma de Buenos Aires, Argentina*
[c] *Frankfurt Institute for Advanced Studies (FIAS), Max-Von-Laue-Strasse 1, 60438 Frankfurt, Germany*
[d] *Department Neurophysiology, Max-Planck-Institute for Brain Research, Deutschordenstrasse 46, 60528 Frankfurt, Germany*
[e] *Instituto de Física Interdisciplinar y Sistemas Complejos, Universitat de les Illes Balears, E-07122 Palma de Mallorca, Spain*

Received 2 May 2007; received in revised form 31 July 2007; accepted 2 August 2007

Available online 12 September 2007

Communicated by C.R. Doering

Abstract

In this Letter, we make use of two information-theory based indicators to measure the goodness of two encryption schemes commonly used within the context of chaotic communications. In particular, we have shown that the computation of the normalized Shannon entropy and the MPR-Statistical Complexity measure [M.T. Martín, A. Plastino, O.A. Rosso, Phys. Lett. A 311 (2003) 126, P.W. Lamberti, M.T. Martín, A. Plastino, O.A. Rosso, Physica A 334 (2004) 119] for different chaotic laser signals can lead to statistically significant criteria to assess the quality of several encryption techniques. The proposed measures allow, in some cases, to detect the presence of a message embedded within a chaotic carrier. They also reveal that the Chaos Modulation scheme is more reliable from the statistical point of view, when compared with the Chaos Shift Keying.

PACS: 42.55.Px; 42.65.Sf; 89.70.+c

Keywords: Signal encryption; Chaos; Semiconductor laser; Entropy; Statistical complexity

1. Introduction

The security aspects of most of nowadays standard cryptographic systems are often estimated on the basis of the computational power that is required to effectively decode an encrypted message. Thus, in digital cryptographic protocols (such as the widely used RSA cipher [1]) the security of the system relies on the fact that even with the most efficient algorithms available today, the inversion of the encryption procedure is an excessively time-consuming task for any practical purpose. However, the potential security of most of the well-known ciphers remains an open problem. For instance, in present time, no mathematical proof is known to demonstrate the non-existence of fast factoring large number algorithms, a procedure whose presumed infeasibility lies at the heart of the RSA performance.

The assessment of the security level for analog encryption protocols has been much less studied in the literature. In this

* Corresponding author at: Chaos & Biology Group, Instituto de Cálculo, Facultad de Ciencias Exactas y Naturales, Pabellón II, Ciudad Universitaria, 1428 Ciudad Autonoma de Buenos Aires, Argentina. Tel./fax: +54 11 4786 8114.
E-mail addresses: oarosso@fibertel.com.ar (O.A. Rosso), raulvicente@mpih-frankfurt.mpg.de (R. Vicente), claudio@ifisc.uib.es (C.R. Mirasso).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2007.08.063

case, the presence of a continuum of states posses some problems which preclude the application of the mathematical apparatus that has been traditionally used for cryptography based on finite fields. In this Letter we propose the computation of two information theory based quantifiers (normalized Shannon entropy and MPR-Statistical Complexity [2,3]) as a possible test of the goodness of different analog encryption schemes. Both quantifiers are complementary in some sense and have proved to be very useful in the characterization of time series from different origin [4–7]. In fact, the normalized Shannon entropy provides a measure of the order/disorder. The MPR statistical complexity quantifies not only randomness but also the presence of correlated structures [2,3]. It should be noticed that the MPR complexity measure *is not a trivial function of the entropy*, in the sense that, for a given entropy value H, there exists a range of possible statistical complexity measure values between a minimum $C_{\min}$ and a maximum $C_{\max}$ [8]. Thus, evaluating the statistical complexity measure provides one with important *additional* information regarding the peculiarities of a probability distribution (see i.e. Refs. [4–7] and references therein).

We focus our attention on chaos encrypted communications. The idea behind chaotic communications is to use the broadband spectrum of a deterministic chaotic carrier to hide a small amplitude message. After propagation through a proper communication channel, the recovery process relies on the selective synchronization by an authorized part to the chaotic component of the transmitted signal. Then, a straightforward comparison of the received and the synchronized signal leads to the message extraction [9].

Information theory offers a proper framework for the statistical evaluation of quantities such as the content, rate of production, and flow of information in univariate and multivariate signals. Here, we take advantage of the ability of these statistical complexity measures to detect and quantify the effect of a message embedded within a chaotic carrier.

Our main goal is to test whether these quantifiers can give some insight to questions such as: (a) which is the optimal sampling frequency that reveals the presence of information masked in a chaotic signal? (b) which is the optimal message amplitude for the encryption/decryption process? or (c) can we discriminate the security level of different encryption schemes?

The Letter is organized as follows. In Section 2 we introduce the basic ideas and methodology to compute the information theory based quantifiers. Section 3 describes the origin and characteristics of the data sets used in our analysis. The results are presented in Section 4 altogether a discussion of their significance. Finally, a summary and conclusions are given in Section 5.

2. Information theory quantifiers

In a recent contribution, López-Ruiz, Mancini and Calbet (LMC) have proposed a statistical complexity measure, based on the notion of "disequilibrium", as a quantifier of the degree of physical structure in a time series [10]. Given a probability distribution P associated to the state of a system, the LMC-measure C_{LMC} is the product of a normalized entropy H (normalized Shannon-entropy) times the disequilibrium Q, given by the Euclidean "distance" from P to the uniform distribution P_e. The statistical complexity vanishes both for a totally random process and for a purely periodic one. Martín, Plastino and Rosso (MPR) [2] improved on this measure by suitably modifying the distance-component (in the concomitant probability space). In Ref. [2], Q is built-up using Wootters' statistical distance [11].

Regrettably enough, the two statistical complexity measures above mentioned are neither intensive nor extensive quantities in the thermodynamical sense, although they yield useful results. Also, a reasonable complexity measure should be able to distinguish among different degrees of periodicity and it should vanish only for the simplest degree of periodicity. In order to attain such goals any natural improvement should give this statistical measure an intensive character. In Ref. [3] Lamberti et al. obtained a MPR-statistical complexity measure that is (i) able to grasp essential details of the dynamics, (ii) an intensive quantity, and (iii) capable of discerning among different degrees of periodicity and chaos. This statistical complexity measure is the one to be employed here to assess the goodness of different chaotic encryption paradigms.

The intensive MPR-statistical complexity measure [3] can be viewed as a functional $C_{\mathrm{JS}}[P]$ that characterizes the probability distribution P associated to the time series generated by the dynamical system under study. It quantifies not only randomness but also the presence of correlational structures [2,3,10]. The intensive MPR-statistical complexity is of the form

$$C_{\mathrm{JS}}[P] = Q_J[P, P_e] \cdot H_S[P], \tag{1}$$

where, to the probability distribution $P = \{p_j;\, j = 1, \ldots, N\}$ with N is the number of possible states of the system under study, we associate the entropic measure

$$H_S[P] = \frac{S[P]}{S_{\max}} = \left(-\sum_{j=1}^{N} p_j \ln(p_j)\right) \Big/ S_{\max}, \tag{2}$$

with $S_{\max} = S[P_e] = \ln N$ ($0 \leqslant H_S \leqslant 1$). $P_e = \{1/N, \ldots, 1/N\}$ is the uniform distribution and S is Shannon's entropy. The disequilibrium Q_J is defined in terms of the extensive Jensen–Shannon divergence [3] and is given by

$$Q_J[P, P_e] = Q_0\big\{S\big[(P + P_e)/2\big] - S[P]/2 - S[P_e]/2\big\}, \tag{3}$$

with Q_0 a normalization constant ($0 \leqslant Q_J \leqslant 1$) given by

$$Q_0 = -2\left\{\left(\frac{N+1}{N}\right)\ln(N+1) - 2\ln(2N) + \ln N\right\}^{-1}. \tag{4}$$

Thus, the disequilibrium Q_J is an intensive quantity. The disequilibrium Q would reflect on the systems's "architecture", being different from zero if there exist "privileged", or "more likely" states among the accessible ones.

For evaluating the probability distribution P associated to the time series (dynamical system) under study we follow the methodology proposed by Bandt and Pompe [12] and consider partitions of the D-dimensional space that will hopefully "reveal" relevant details of the ordinal-structure of a given

one-dimensional time series. Given the time-series $\{x_t : t = 1, \ldots, M\}$ and an embedding dimension $D > 1$ and time lag $\tau = 1$, we are interested in "ordinal patterns" of order D [12–14] generated by

$$(s) \mapsto \big(x_{s-(D-1)}, x_{s-(D-2)}, \ldots, x_{s-1}, x_s\big), \tag{5}$$

which assigns to each time s the D-dimensional vector of values at times $s, s-1, \ldots, s-(D-1)$. Clearly, the greater the D-value, the more information on the past is incorporated into our vectors. By the "ordinal pattern" related to the time (s) we mean the permutation $\pi = (r_0, r_1, \ldots, r_{D-1})$ of $(0, 1, \ldots, D-1)$ defined by

$$x_{s-r_{D-1}} \leqslant x_{s-r_{D-2}} \leqslant \cdots \leqslant x_{s-r_1} \leqslant x_{s-r_0}. \tag{6}$$

In order to get a unique result we set $r_i < r_{i-1}$ if $x_{s-r_i} = x_{s-r_{i-1}}$. Thus, for all the $D!$ possible permutations π of order D, the probability distribution $P = \{p(\pi)\}$ is defined by

$$p(\pi) = \frac{\sharp\{s | s \leqslant M - D + 1; (s),\ \texttt{has type}\ \pi\}}{M - D + 1}. \tag{7}$$

In this expression, the symbol $\sharp$ stands for "number". The normalized entropy H_S and the intensive MPR-statistical complexity C_{JS} are then evaluated for this "permutation" probability distribution.

The method proposed by Bandt and Pompe [12] for evaluating the probability distribution P is based on the details of the attractor-reconstruction procedure. Bandt and Pompe consider a partition of the D-dimensional state space determined by the intersections of $D!$ hyper-planes of $\mathbb{R}^D$: $x_1 = x_2, \ldots, x_1 = x_D; x_2 = x_3, \ldots, x_2 = x_D; \ldots; x_{D-1} = x_D$. Each permutation π of order D can be associated with one of the connected pieces determined by the partition. In other words an "ordinal pattern" represents one connected piece of $\mathbb{R}^D$, and the union of all pieces is the total state space $\mathbb{R}^D$. The probability distribution P of "ordinal patterns" is given by the frequency, in the attractor structure, of each piece (pattern). P is assigned by "counting" the times that the attractor visits each piece (see Eq. (7)). In particular, if the attractor is symmetric with respect to the hyperplanes, all the connected pieces have the same frequency and thus the distribution of ordinal patterns is uniform: the attractor "visits" all the partition pieces with the same frequency. Consequently, the information provided by the time series so as to predict geometric locations of successive D-strings vanishes and the entropy is maximal ($S_{\max} = \ln D!$ and $H_S = 1$). On the other hand, if the situation is such that the attractor remains always within just one of the connected pieces, one can "predict" with certainty $H_S = 0$.

The advantages of Bandt and Pompe' method reside in (a) its simplicity, (b) the associated extremely fast calculation-process, (c) its robustness, and (d) its invariance with respect to nonlinear monotonous transformations. The Bandt and Pompe's methodology can be applied to any type of time series (regular, chaotic, noisy, or reality based), with a weak stationary assumption [12]. It is important to remark that for the applicability of Bandt and Pompe's technique we need not to assume that the time series under analysis is representative of low-dimensional dynamical systems. In this methodology the embedding dimension D plays an important role in the evaluation of the appropriate probability distribution. This is so because D determines the number of accessible states $D!$ Also, it conditions the necessary length M of the time series that one needs in order to work with a reliable statistics. In relation to this last point, we propose that the condition $M \gg D!$ has to be satisfied. This relation is followed immediately taken into account that $(M - D + 1)$ is the total number of points (vectors) in the reconstructed phase space. In particular, Bandt and Pompe suggest for practical purposes to work with $3 \leqslant D \leqslant 7$ with time lag $\tau = 1$.

3. Data description

The data under consideration correspond to numerical simulations of a well-established semiconductor laser model subject to coherent optical feedback; the Lang–Kobayashi model [15]. Under appropriate conditions of feedback strength and time delay this type of laser enters into a high-dimensional chaotic regime known as Coherence Collapse (see Ref. [16] for a detailed analysis of the dimensionality and the Kolmogorov–Sinai entropy measure of this chaotic regime as a function of several laser parameters). The generated chaotic varying signal can be used as the carrier in which a small amplitude digital message can be hided. An extensive review on optical chaos and applications to cryptography can be found in Refs. [17,18]. Here, we focus on the encryption of a pseudo-aleatory message within such a chaotic carrier by means of two different techniques; Chaos Shift Keying (CSK) [19] and Chaos Modulation (CM) [9]. In the first one, a message is introduced in the chaotic carrier by slightly perturbing one of the parameters of the laser such as the injection current. On the other hand, the CM technique provides a suitable embedding of the message within a chaotic series by a weak modulation of the output accordingly to the message signal.

Each time series here analyzed contains $N = 5 \times 10^6$ points representing the intensity of the laser output. Three different sampling period values are considered $\Omega_s = 1, 10, 100$ ps. Amplitudes ranging from $A = 0\%$ to 20% of a given reference value are studied for the two encryption methods; the CSK and CM. The message applied in all cases follows a pseudo-aleatory binary distribution.

4. Results and discussion

For the evaluation of the information theory based quantifiers (normalized entropy H_S and intensive MPR-statistical complexity C_{JS}) each time series is divided in disjoint sections of $M = 10^4$ points. For each portion the distribution of permutation probabilities is determined considering an embedding dimension of $D = 6$ while the time lag is chosen to be $\tau = 1$. Once the probability distribution is known the application of Eqs. (1) and (2) leads to the corresponding values of H_S and C_{JS}. Note that the condition $M \gg D!$ is always satisfied and consequently, statistically significant distribution probabilities are expected.

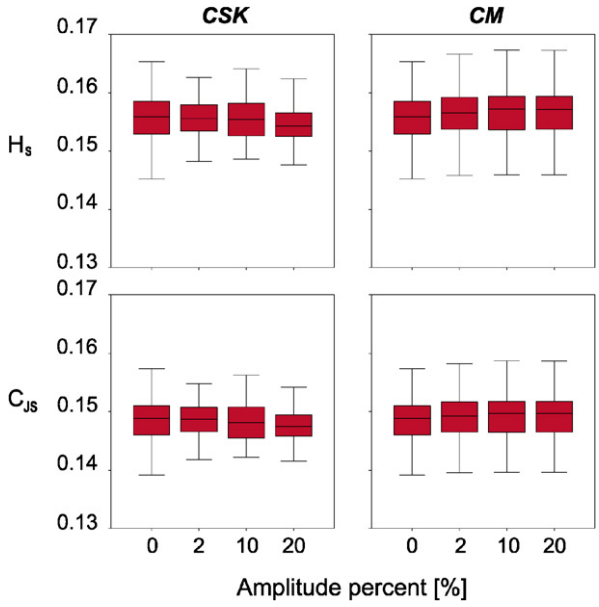

Fig. 1. Normalized entropy, H_S, and intensive MPR-statistical complexity, C_{JS}, boxplots for different amplitude message percent and sample time $\Omega_s = 1$ ps. Left and right column correspond to the Chaos Shift Keying (CSK) and Chaos Modulation (CM) encryption techniques respectively. Horizontal lines represent the ANOVA results highly significant ($p \leqslant 0.001$).

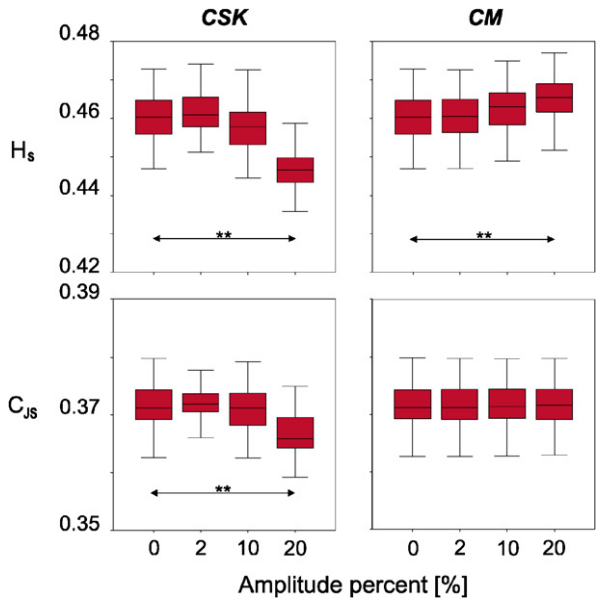

Fig. 2. Same as Fig. 1 for sample time $\Omega_s = 10$ ps.

The obtained results (boxplots) for the two quantifiers (entropy and complexity) are shown in Figs. 1 to 3 and correspond to the three time samples $\Omega_s = 1, 10, 100$ ps respectively. As usual, boxplots [20] illustrate lower and upper lines at the lower quartile (25th percentile of the sample) and upper quartile (75th percentile of the sample), respectively, while the line in the middle of the box is the sample median. The whiskers are lines extending from each end of the box indicating the extent of the rest of the sample.

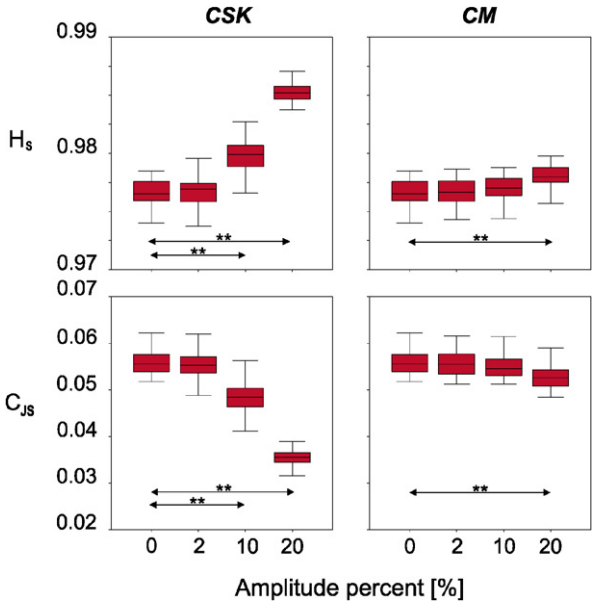

Fig. 3. Same as Fig. 1 for sample time $\Omega_s = 100$ ps.

4.1. Encryption tests

We compare the mean values of the quantifiers H_S and C_{JS} as a function of the amplitude used to encode the messages. One-way ANalysis Of VAriance (ANOVA) together posthoc tests with Sheffe multiple comparisons [20] are used to test if the mean value of the complexity measures for different amplitudes are statistically different (level of significance $p = 0.05$). In particular, we are interested if such statistical difference is found when comparing the pure chaotic carrier ($A = 0\%$) to non-zero amplitude message data sets ($A \neq 0\%$). If so, the present procedure would provide a fast algorithm to detect the presence of a hidden message in a chaotic carrier. The comparison of the mean values corresponding to the Information Theory based quantifiers between the different encoding schemes will also be investigated as well as the influence of the sampling time (Ω_s).

4.2. Results

Following the order of the questions settled on the introductory section, we start our analysis by looking at the effects that different sampling periods can produce on the entropy and the complexity measures and their relation to the message masking. Both quantifiers H_S and C_{JS} present relevant variations according to the degree of detail in the description of the system under study. The two measures here estimated are then cross-graining dependents. For a discussion of this effect on two-dimensional spatial patterns see Ref. [21]. In the case of one-dimensional time series generated by a continuous dynamical system the cross-graining effects are evidenced by changing the sample time. As an example, consider the well known Lorenz system given by three ordinal differential equations (ODEs) [22], with parameters set: $\sigma = 16$, $B = 4$ and $R = 45.92$ which correspond to a chaotic dynamics. Entropy and complexity were evaluated for the corresponding time series ($M = 32768$ data

Table 1
Normalized Shannon Entropy, H, and MPR-statistical complexity, C_{JS}, obtained with BP methodology ($D = 6$, $\tau = 1$) for the time series ($M = 32768$ data samples) corresponding to the X-coordinate of the Lorenz system obtained by integration of the three ODEs with chaotic behavior and different integration time steps ΔT

ΔT	H	C_{JS}
0.01	0.210	0.197
0.10	0.695	0.453
1.00	0.967	0.076

points) obtained by integration (fourth-order Runge–Kutta of with variable step) of the ODEs for the followings time steps (sampling time) $\Delta T = 0.01, 0.10$ and 1.00. The obtained values for the X-variable and $D = 6$ are given in Table 1. The typical value used in the literature is $\Delta T = 0.1$ which gives in principle a "correct" sampling of the dynamics under study, and the values of the H and C_{JS} can be taken of representative of this behavior. The other two values clearly represent oversampling and subsampling of the dynamics and their effect on the numerical values of the quantifiers is clear (see Table 1). In fact, these quantifiers could be consider as indicators of the best sampling time in order to correct capture the systems dynamics. Deeper works in this direction are in progress.

Figs. 1 to 3 show a clear dependence of the entropy and the complexity measures as a function of the sampling time Ω_s of our laser time series, i.e. the temporal resolution at which we are looking at the signal. We can observe that for all message amplitudes studied $A = 2\%$, 10% and 20% there is a systematic increment of H_S while enlarging the sampling period. At this point, it is important to remind the existence of two relevant time scales in the time series. One is the typical correlation time of the chaotic carrier ($\tau_c \sim 40$ ps), while the other is the duration of a message bit ($T = 1000$ ps). For $\Omega_s = 1$ ps ($\ll \tau_c$), there is an oversampling of the dynamics of the recorded time series which leads to low values for the normalized entropy and complexity measures. On the other hand, subsampling at times far beyond the correlation time induces a randomization of the chaotic signal and high entropy values are reported (high degree of disorder). Accordingly, the subsampled chaotic series reveal their noise-like properties by throwing an almost null value for the complexity due to the closeness of the computed permutation probabilities to a uniform distribution. Sampling values of the order of the dynamics time scale provide a more representative structure of the signal and leads to intermediate values for H_S and C_{JS}.

Perhaps more interesting is the fact that the ability of the algorithm to detect the presence of a message crucially depends on the sampling time. Thus, Fig. 3 reveals that for both encryption schemes a sampling time of $\Omega_s = 100$ ps is the best to discriminate a message-container signal from a pure chaotic carrier. For such a sampling period the ANOVA analysis of the CSK encoding detects highly significant ($p \leqslant 0.001$) differences in the mean value of entropy and complexity corresponding to time series encrypted with $A = 10\%$ and 20% amplitude message when compared to pure carriers. Messages with amplitude $A = 2\%$ are statistically indistinguishable from signals which contain no message at all. For the CM scheme amplitudes as large as $A \geqslant 20\%$ are needed in order to produce a significant effect on the entropy and complexity values to be statistically distinguishable.

When shortening the sampling period one finds that the entropy and complexity measures provide very similar values for different message amplitudes. This turns out in a reduced functionality of these statistical quantifiers as message detectors even when the dynamics of the signal is better resolved. One possible explanation for such behavior is that the main effects of the introduction of a digital message within a chaotic carrier occur at the transition between two different bits. It is at those borders, when the message is changing its value in a discrete manner, where it is more probable that the message can modify the ordinal structure of the chaotic signal and disturb the natural permutation probability distribution. Consequently, an oversampling of the signal by including more data points where no message transition is occurring might tend to wash out the effect of the message in our statistical measures. Taking into account that $T = 1000$ ps is the duration of message bit, it is clear that from our three sampling times $\Omega_s = 100$ ps is the optimum for statistically describe those effects as observed in Fig. 3.

In summary we have found that for $\Omega = 100$ ps, our entropy and complexity quantifiers are more sensitive to the presence of a message within the chaotic carrier. In this case, the sampling time is larger than the correlation time of the chaotic carrier (we calculated the correlation time to be around 40 ps) and thus the sampling procedure induces a randomization of the signal which can be observed from the fact that the entropy and complexity measures approach to 1 and 0, respectively, which are the theoretical values for pure stochastic processes. This generalizes to sampling times larger than correlation time of the carrier. However, sampling time of $\Omega = 1000$ ps was not included in the manuscript since it coincides with the duration of a bit of the modulated message; in order to capture the structure of the message (which was the signal to detect within the chaotic background) we work sampling times smaller than the duration of a bit.

The chaotic carrier and the modulated message contribute differently to the entropy and complexity measures as mentioned above. The larger contribution of the message to the unpredictability of the whole signal occurs at the edges between different bits. Thus, it is expected that oversampling the signal while the message is at a constant level (this is during the duration of a bit) does not effectively contribute much to reveal the presence of the message (washing out). One could expect, in principle, some changes in the time series when the message is present. We have checked that a simple observation of the time series does not reveal us any information about the effect of the sampling in the detectability of the message (correlation analysis of signals with different sampling times were also ineffective in such task). However, if we compare Figs. 1, 2, and 3 it is clear that there is an increase of detectability of the message with our quantifiers when changing the sampling time. Fig. 1 ($\Omega = 1$ ps) shows a clear insensitivity in the quantifiers to the presence of any message while Fig. 3 (for sampling times of

$\Omega = 100$ ps) shows the best detectability. This indicates that the sampling time is critical to capture the structure of the message within the carrier and that this increment in sensitivity cannot come from the chaotic background contribution whose effect is just to bias the values of the entropy and complexity to 1 and 0, respectively. Thus, the change in the sensitivity (or "slope" of the graphics) from Figs. 1 to 3 is associated to the effect of the sampling relative to the duration of the message bit.

The characteristics of the encryption/decryption process in chaos based communications impose some conditions on the election of the amplitude to encode a message. On one hand, it should be small enough to avoid simple attacks, e.g. unmasking by attractor reconstruction techniques, and on the other hand it must be large enough to ensure an efficient recovery of the message by the synchronization to an authorized system. In our case, when $A = 2\%$ independently of the encoding technique and sampling time the complexity and entropy measures are unable to detect any statistical difference due to the presence of the message. For the value of $A = 10\%$ the difference is not detected 66.67% of the cases for the CSK coding and 100% for the CM. Amplitude $A = 20\%$ causes these values drop down to 33.33% and 50%, respectively. This is, for the same amplitude messages encoded with CM are more difficult to detect. Based on these results and the fact that a proper deciphering by selective synchronization can be performed for amplitudes as small as $A \sim 2\%$, we consider that a CM masking at that amplitude provides an optimum encryption scheme from the perspective of information theory.

5. Conclusions

We have proposed the computation of two measures based on information theory grounds to assess the performance of different chaotic encryption schemes. In particular, a disorder and a complexity quantifiers (normalized Shannon entropy and intensive MPR-Statistical Complexity) are evaluated for different time series generated by a chaotic laser in which a message is encrypted. ANOVA analysis has proved that both measures successfully detect the presence of a message provided that a message amplitude larger than 10% and the proper sampling time are used. On the contrary, we observe that message amplitudes smaller than 10% are almost undetectable for both CSK and CM encryption schemes although CM appears to be more secure. The statistical measures presented here offer criteria to decide for optimum encoding techniques. The application of these measures to explore and quantify the complexity of synchronized chaotic lasers at different regimes and interacting topologies is considered for future research. The proposed quantifiers have not any restriction in its applicability to the kind of time series, and then the advanced methodology in this paper could work also in the case of data generated by digital chaotic carriers.

Acknowledgements

The authors thank Pablo Salgado for helpful evaluation of ANOVA tests and its discussion. This work was partially supported by the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina (PIP 5687/05, PIP 6036/05) and ANPCyT, Argentina (PICT 11-21409/04). Also it is partially supported by the Spanish MCyT and Feder under project FIS2004-00953, and by EU Project PICASSO IST-2005-34551. O.A.R. gratefully acknowledge support from Australian Research Council (ARC) Centre of Excellence in Bioinformatics, Australia.

References

[1] R. Rivet, A. Shamir, L. Adleman, Commun. ACM 21 (1978) 120.
[2] M.T. Martín, A. Plastino, O.A. Rosso, Phys. Lett. A 311 (2003) 126.
[3] P.W. Lamberti, M.T. Martín, A. Plastino, O.A. Rosso, Physica A 334 (2004) 119.
[4] O.A. Rosso, M.T. Martín, A. Figliola, K. Keller, A. Plastino, J. Neurosci. Methods 153 (2006) 163.
[5] H.A. Larrondo, M.T. Martín, C.M. González, A. Plastino, O.A. Rosso, Phys. Lett. A 352 (2006) 421.
[6] L. Zunino, D.G. Perez, M.T. Martín, A. Plastino, M. Garavaglia, O.A. Rosso, Phys. Rev. E 75 (2007) 021115.
[7] A.M. Kowalski, M.T. Martín, A. Plastino, O.A. Rosso, Physica D (2007), in press.
[8] M.T. Martín, A. Plastino, O.A. Rosso, Physica A 369 (2006) 439.
[9] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C.R. Mirasso, L. Pesquera, K.A. Shore, Nature 438 (2005) 343.
[10] R. López-Ruiz, H.L. Mancini, X. Calbet, Phys. Lett. A 209 (1995) 321.
[11] W.K. Wootters, Phys. Rev. D 23 (1981) 357.
[12] C. Bandt, B. Pompe, Phys. Rev. Lett. 88 (2002) 174102.
[13] K. Keller, H. Lauffer, Int. J. Bifur. Chaos 13 (2003) 2657.
[14] K. Keller, M. Sinn, Physica A 356 (2005) 121.
[15] R. Lang, K. Kobayashi, IEEE J. Quantum Electron. 16 (1980) 347.
[16] R. Vicente, J.L. Dauden, P. Colet, R. Toral, IEEE J. Quantum Electron. 16 (2004) 347.
[17] S. Donati, C. Mirasso (Eds.), IEEE. J. Quantum Electron. 38 (2002) 1138.
[18] L. Larger, J.-P. Goedgebuer (Eds.), C. R. Acad. Sci.-Dossier Phys. 5 (2004) 609.
[19] C.R. Mirasso, J. Mulet, C. Masoller, Phot. Tech. Lett. 14 (2002) 456.
[20] D.C. Montgomery, Design and Analysis of Experiments, John Willy & Sons, New York, 1996.
[21] P. Grassberger, Helvetica Phys. Acta 62 (1989) 498.
[22] H.G. Schuster, Deterministic Chaos, second ed., VCH, Weinheim, 1988.