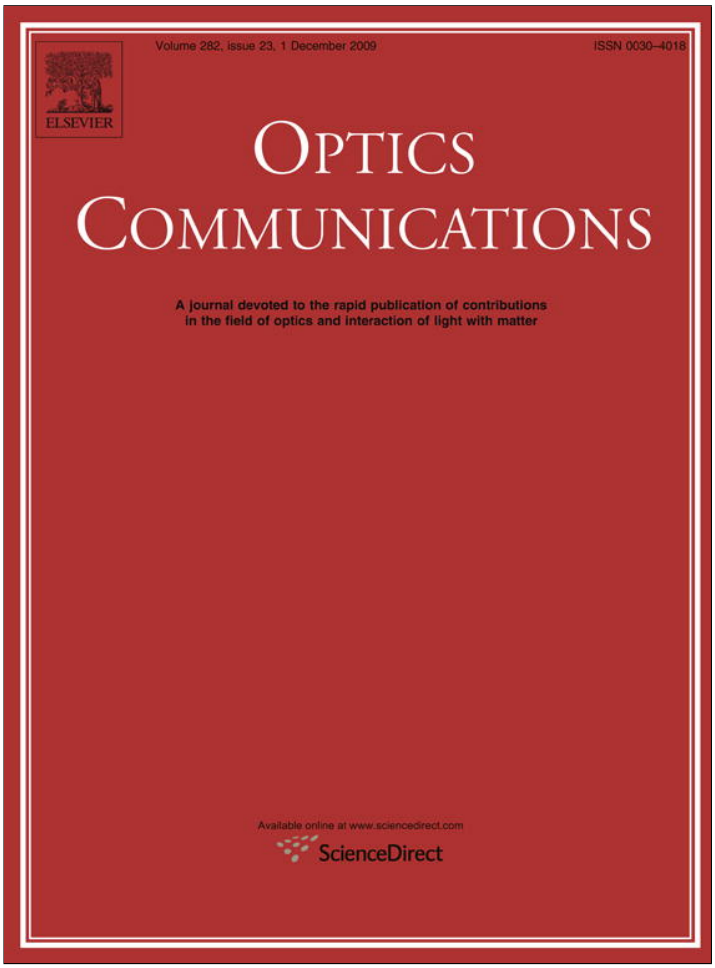

Optics Communications 282 (2009) 4587–4594

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Performance of encryption schemes in chaotic optical communication: A multifractal approach

Luciano Zunino [a,b,c,*], Miguel C. Soriano [d], Alejandra Figliola [e], Darío G. Pérez [f], Mario Garavaglia [a,c], Claudio R. Mirasso [d], Osvaldo A. Rosso [g,h]

[a] Centro de Investigaciones Ópticas, C.C. 3, 1897 Gonnet, Argentina
[b] Departamento de Ciencias Básicas, Facultad de Ingeniería, Universidad Nacional de La Plata (UNLP), 1900 La Plata, Argentina
[c] Departamento de Física, Facultad de Ciencias Exactas, Universidad Nacional de La Plata, 1900 La Plata, Argentina
[d] Instituto de Física Interdisciplinar y Sistemas Complejos (IFISC) CSIC-UIB, Campus Universitat de les Illes Balears, E-07122 Palma de Mallorca, Spain
[e] Chaos and Biology Group, Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, Campus Universitario, Modulo 5, Juan Maria Gutierrez 1150, Los Polvorines, Provincia de Buenos Aires, Argentina
[f] Instituto de Física, Pontificia Universidad Católica de Valparaíso (PUCV), 23-40025 Valparaíso, Chile
[g] Centre for Bioinformatics, Biomarker Discovery and Information-Based Medicine, Hunter Medical Research Institute, School of Electrical Engineering and Computer Science, The University of Newcastle, University Drive, Callaghan NSW 2308, Australia
[h] Chaos and Biology Group, Instituto de Cálculo, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Pabellón II, Ciudad Universitaria, 1428 Ciudad de Buenos Aires, Argentina

ARTICLE INFO

Article history:
Received 10 April 2009
Received in revised form 2 July 2009
Accepted 20 August 2009

PACS:
42.55.Px
42.65.Sf
05.45.Df

Keywords:
Signal encryption
Chaos
Semiconductor laser
Multifractal detrended fluctuation analysis
Hurst exponent
Multifractality degree

ABSTRACT

From the estimation of the Hurst exponent and the multifractality degree we discriminate the security levels of two typical encoding schemes usually applied in chaos-based communication systems. We also analyze the effects that the sampling period and the message amplitude have on the goodness of these techniques. We compare our results with those obtained by considering an information theory approach [O.A. Rosso, R. Vicente, C.R. Mirasso, Phys. Lett. A 372 (2007) 1018]. The Hurst exponent seems to be a sensitive and powerful tool for discriminating the presence of a message embedded in a chaotic carrier.

1. Introduction

Chaotic optical communication is a hot topic nowadays [1–6]. It tries to improve and complement software or quantum cryptography, introducing a second level of security. The standard chaotic optical communication system is based on a pair of synchronized semiconductor lasers, in which a transmitter generates chaotic optical carrier for embedding the transmitted message, and a receiver laser duplicates the chaotic carrier and filters out the encoded message. The transmitted message can be recovered after a straightforward comparison of the received and the synchronized signals. The main idea is to use the broad bandwidth (typically in the 10–100 GHz range) and the high dimension of the optical chaos to hide a small amplitude message. Argyris et al. have demonstrated high-speed communication based on chaos synchronization over 120 km of commercial fibre-optic channel in the metropolitan area network of Athens, Greece. Transmission rates in the gigabit per second range and bit-error rates as low as 10^{-7} were achieved [7]. It is clear that the bit-error rate is determined by the synchronization condition, i.e., by the parameter matching between both lasers. However, it was recently shown that the quality of the recovered message also depends on the filtering

* Corresponding author. Address: Centro de Investigaciones Ópticas, C.C. 3, 1897 Gonnet, Argentina. Tel.: +54 221 4714341; fax: +54 221 4717872.
E-mail addresses: lucianoz@ciop.unlp.edu.ar (L. Zunino), miguel@ifisc.uib-csic.es (M.C. Soriano), afigliol@ungs.edu.ar (A. Figliola), dario.perez@ucv.cl (D.G. Pérez), garavagliam@ciop.unlp.edu.ar (M. Garavaglia), claudio@ifisc.uib-csic.es (C.R. Mirasso), oarosso@fibertel.com.ar (O.A. Rosso).

0030-4018/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2009.08.047

characteristics of the receiver [3] and the amplitude of the embedded message [8]. For an exhaustive review about synchronization of chaotic oscillations in semiconductor lasers with optical feedback and its application to secure communications see Refs. [9–11].

Based on the semiconductor laser rate equations subject to low to moderate optical feedback (Lang–Kobayashi model [12]) we numerically analyze the performance of conventional encryption schemes within the context of the chaos-based communication systems. For that purpose we estimate the Hurst exponent and multifractality degree of the numerical time series by using the multifractal detrended fluctuation analysis introduced in the pioneering work of Castro e Silva and Moreira [13] and developed more recently by Kantelhardt et al. [14]. This robust and powerful technique identifies and, more importantly, quantifies the multiple scaling exponent within a time series. It has been successfully applied in a variety of different scientific fields, like seismology [15], cardiac dynamics [16], solar dynamics [17], laser propagation in turbulent media [18], music [19], epileptic EEG time series [20], air temperature fluctuations [21], traffic time series [22], color series of paintings [23], financial markets [24], river flows [25] and random multiplicative process [26], to study multifractality. Furthermore, several descriptors derived from the multifractal theory were introduced to characterize or distinguish system dynamics [18,21,24,27–33]. Particularly, the two quantifiers mentioned above, the Hurst exponent and the multifractality degree, have been recently used to characterize the stage of market development of world stock indices [34]. We extrapolate this idea and use these indicators to measure the efficiency of the encryption schemes.

The main goal of this work is to estimate the performance, in terms of security, of two well-known encryption schemes: chaos modulation (CM) and chaos shift keying (CSK). Although it would be desirable to directly extract the message it is always important to know in advance whether any information is hidden or not into the chaotic carrier, especially in those cases where multiple chaotic signals are being transmitted simultaneously. This initial test would also prevent the extra effort required to extract the message in case the latter is not present in the carrier. So, it should be stressed that when we talk about encryption efficiency we are referring to the ability of the scheme to hide the presence of the message. In this sense, our work aims to provide an upper bound for the message amplitude in terms of encryption purposes. With this in mind, we tackle the same questions introduced by Rosso et al. [35]: (i) which is the optimal sampling frequency that reveals the presence of information masked in a chaotic signal? (ii) which is the optimal message amplitude? and (iii) can we distinguish the security degree of different encryption techniques?

The remainder of this paper is organized as follows. In Section 2 we describe the multifractal detrended fluctuation analysis required for a proper understanding of the methodology used to estimate our two quantifiers, the Hurst exponent and multifractality degree. In Section 3, the data used in this study are detailed. In Section 4 we present and discuss the results, and, finally, in Section 5, some concluding remarks are given.

2. Multifractal methodology

The standard partition function multifractal formalism (see Chapter 6 of Ref. [36]) was developed for stationary time series. Thus, it does not give correct results for non-stationary time series. The wavelet transform modulus maxima (WTMM) method [37] was introduced to analyze strongly non-stationary data.

More recently, Kantelhardt et al. [14] developed a method for the multifractal characterization of non-stationary time series, which is based on a generalization of the detrended fluctuation analysis (DFA) [38]: the multifractal detrended fluctuation analysis (MFDFA). It has been shown that for short series and negative moments, the significance of the results for the MFDFA is better than for the WTMM method [14]. It has also been concluded that the MFDFA should be recommended for a global detection of multifractal behavior [39]. Moreover, the implementation of the MFDFA does not involve more effort than the conventional DFA. It just requires one additional step. Due to these reasons, we have chosen the latter for a proper detection of the multifractality of the data we aim to analyze.

The MFDFA can be summarized as follow [14]:

- *Step 1.* Starting with a time series (signal) $\{u_i, i = 1, \ldots, N\}$, where N is the length of the series, the corresponding profile is determined by

$$Y(k) = \sum_{i=1}^{k} [u_i - \langle u \rangle], \quad k = 1, \ldots, N, \tag{1}$$

  where $\langle \cdot \rangle$ denotes the averaging over the whole time series.
- *Step 2.* The profile $Y(k)$ is divided into $N_s \equiv [N/s]$ non-overlapping windows of equal length s. Since the record length N does not need to be a multiple of the considered time scale s, a short part at the end of the profile will remain in most cases. In order to take into account this part of the record, the same procedure is repeated starting from the other end of the recorded series. Thus, $2N_s$ windows are obtained.
- *Step 3.* The local trend for each window $v = 1, \ldots, 2N_s$ is evaluated by least-square fit of the data. The detrended time series for the window length s, denoted by $Y_s(i)$, is calculated as the difference between the original time series and the fits,

$$Y_s(i) = Y[(v-1)s + i] - p_v(i), \tag{2}$$

  for $v = 1, \ldots, N_s$, and

$$Y_s(i) = Y[N - (v - N_s)s + i] - p_v(i), \tag{3}$$

  for $v = N_s + 1, \ldots, 2N_s$. Here, $p_v(i)$ is the fitting polynomial in the vth window. Since the detrending of the time series is done by subtraction of the fits from the profile, these methods differ in their capability of eliminating trends in the data. In mth order of MFDFA, trends of order m in the profile and $m-1$ in the original record are eliminated. Thus, a comparison of the results for different orders of MFDFA allows to estimate the polynomial trend in the time series. Since we use a polynomial fit of order 3, we denote the algorithm as MFDFA-3.
- *Step 4.* For each of the $2N_s$ segments the second moment of the detrended time series $Y_s(i)$ is evaluated by averaging over all data points i in the vth window

$$F_s^2(v) = \frac{1}{s} \sum_{i=1}^{s} (Y_s(i))^2. \tag{4}$$

- *Step 5.* The qth order fluctuation function is obtained by averaging over all segments

$$F_q(s) = \left\{ \frac{1}{N_s} \sum_{v=1}^{N_s} \left[F_s^2(v) \right]^{q/2} \right\}^{1/q}, \tag{5}$$

  starting from the beginning, and

$$F_q(s) = \left\{ \frac{1}{N_s} \sum_{v=N_s+1}^{2N_s} \left[F_s^2(v) \right]^{q/2} \right\}^{1/q}, \tag{6}$$

  starting from the end. The order q can take any real value. However, for $q = 0$ the average procedure described by Eqs. (5) and (6) cannot be applied because of the diverging exponent. In-

stead, a logarithmic average procedure has to be employed [14]. For $q = 2$, the standard DFA procedure is retrieved.

- *Step 6.* Finally, the scaling behavior of the fluctuation is determined by analyzing log–log plots of $F_q(s)$ versus s for each value of q. If the series u_i are long-range correlated $F_q(s)$ increases, for large values of s, as a power-law

$$F_q(s) \sim s^{h(q)}. \tag{7}$$

For monofractal time series with compact support, $h(q)$ is independent of q, since the scaling behavior of the variance $F_s^2(v)$ is identical for all segments v, and the averaging procedure will give just this identical scaling behavior for all values of q. Only if small and large fluctuations scale differently, there will be a significant dependence of $h(q)$ on q. If we consider positive values of q, the segments v with large variance $F_s^2(v)$ will dominate the average $F_q(s)$. Thus, for positive values of q, $h(q)$ describes the scaling behavior of the segments with large fluctuations. On the contrary, for negative values of q, the segments v with small variance $F_s^2(v)$ will dominate the average $F_q(s)$. Hence, for negative values of q, $h(q)$ describe the scaling behavior of the segments with small fluctuations. Obviously, richer multifractality corresponds to higher variability of $h(q)$. The multifractality degree is estimated from

$$\Delta h = \max_q[h(q)] - \min_q[h(q)]. \tag{8}$$

This value quantifies the complexity of the data [29,32]. The broader this range, the richer the structure of the system under study. By using this broadness measure we compare the structural richness of the different available data sets. We guess that a chaotic carrier with an embedded signal is structurally richer than the carrier alone and, therefore, the multifractality degree is expected to be larger in the former case. So, this quantifier should be able to detect the presence of a message and it can be used as an efficiency measure of encryption schemes.

Another representative parameter of the multifractal analysis is the well-known Hurst exponent H. It was originally introduced within the Hurst's rescaled range analysis (R/S analysis) [40] as a measure of the correlation in time series. Mandelbrot and Van Ness used this parameter, bounded to the range $(0, 1)$, within the fractional Brownian motion stochastic model [41]. These processes exhibit memory for any Hurst exponent except $H = 1/2$. In this case successive Brownian motion increments are as likely to have the same sign as the opposite, and thus there is no correlation. When $H > 1/2$ the correlations of successive increments decay hyperbolically, and this sub-family of processes have long-memory. Besides, consecutive increments tend to have the same sign, these processes are persistent. For $H < 1/2$, the correlations of the increments also decay but exponentially, and this sub-family presents short-memory. Since consecutive increments are more likely to have opposite signs, it is said that these are anti-persistent. For a stationary time series such as the fractional Gaussian noise, the profile defined in Eq. (1) will be a fractional Brownian motion. Thus, $0 < h(2) < 1$ for these processes, and $h(2)$ is identical to the Hurst exponent. On the other hand, if the original signal is a fractional Brownian motion, the profile will be a sum of a fractional Brownian motion, so $h(2) > 1$. In this case the relationship between the exponent $h(2)$ and the Hurst exponent H is $H = h(2) - 1$. See Ref. [17] for further details. For these reasons the exponent $h(q)$ is usually known as the generalized Hurst exponent.

One of us (A. Figliola) has recently shown that the MFDFA is robust for detecting multifractality in time series corrupted by additive white noise [42]. It was found that uncorrelated noise does not affect the shape and location of the multifractal spectrum estimated via the MFDFA. However, in the case of correlated or anti-correlated noises this multifractal spectrum is narrower than the spectrum without noise and it is centered in the Hurst exponent value of the noise. It is clear that real-world data are naturally contaminated by uncorrelated noise. So, the MFDFA can be considered reliable for the multifractal quantification of noisy real data.

It should be stressed that it is not intention of this work to relate the physical system under analysis with a fractional Brownian motion stochastic model. Following the same line of reasoning recently introduced by Chlouverakis and co-workers [43] we use the Hurst exponent H as a numerical estimation tool for quantifying the predictability of a time series. This parameter has also been introduced by Lam et al. [44] to study the phase fluctuations dynamic of semiconductor lasers with optical feedback. It is found that the Hurst exponent, estimated from experimental and numerical time series, grows from 0.5 to about 0.7 as the feedback strength is increased.

3. Data description

The chaotic carrier of the data under analysis correspond to numerical integration of the Lang–Kobayashi equations [12]. These widely used equations model a semiconductor laser subject to coherent optical feedback. More precisely, we consider a laser in the coherence collapse regime with moderate feedback values, where the laser exhibits chaotic fluctuations [45]. The equations for the complex slowly varying amplitude of the electric field $E(t)$ and the carrier number inside the cavity $N(t)$ read

$$\dot{E}(t) = \frac{1+i\alpha}{2}\left[G(t) - \frac{1}{\tau_p}\right]E(t) + \gamma E(t-\tau)e^{-i\Phi}, \tag{9}$$

$$\dot{N}(t) = \frac{I}{e} - \frac{N(t)}{\tau_N} - G(t)P(t), \tag{10}$$

where $G(t) = g(N(t) - N_0)/(1 + sP(t))$ is the optical gain, $P(t) = |E(t)|^2$, $\alpha = 5$ is the linewidth enhancement factor, $\tau_p = 2$ps is the photon lifetime, $\tau_N = 2$ ns is the carrier lifetime, $g = 1.5 \times 10^{-8}$ ps^{-1} is the differential gain coefficient, $N_0 = 1.5 \times 10^8$ is the carrier numbers at transparency, $s = 5 \times 10^{-7}$ is the gain compression coefficient, $\tau = 1$ ns is the feedback delay time, $\gamma = 20$ ns^{-1} is the feedback strength, $\Phi = 0$ is the optical feedback phase and e is the electron charge. The pump current is fixed to $I = 1.5I_{th}$ with $I_{th} = 14.7$ mA the threshold current.

Different encryption schemes have been proposed to encode the message within the chaotic carrier: amplitude chaos masking (ACM), chaos modulation (CM) and chaos shift keying (CSK), without being exhaustive[1]. In the first technique the message is directly added to the carrier signal. In the second one the amplitude carrier is weakly modulated by the message. Finally, in the CSK scheme the message is introduced in the chaotic carrier by slightly perturbing the injection current of the laser [48]. In all these methods, the intensity of the message should be small enough in order to avoid detection in the time or frequency domains. In this work we focus our comparative analysis on the CM and CSK encryption schemes; they are widely used and easy to implement experimentally. Moreover, they have been found to be more secure than ACM.

Time series representing the intensity of the laser output were numerically integrated using a second-order Runge-Kutta method with a time step of $\Delta t = 0.1$ ps. We analyzed time series with $N = 5 \cdot 10^5$ data points for three different sampling periods $\Omega_s = 1, 10, 100$ ps and message amplitude ranging from $A = 0\%$ to 20% of a given reference were considered. The hidden message follows a pseudo-random binary distribution in all cases and the duration of a message bit was 1000 ps.

[1] It should be stressed that alternatives in the message encryption have been recently introduced [2,46,47].

4. Results and discussion

We have estimated the scaling exponents $h(q)$ via the MFDFA-3 procedure. Each time series was divided in non-overlapping sets of 5×10^3 data points. Thus, we have 100 different realizations for each configuration of scheme, sampling period and message amplitude. In our analysis q runs from -20 to 20 with a step of 1 and the window lengths, s, is between 10 and $N/4$ with a step of 4, where N

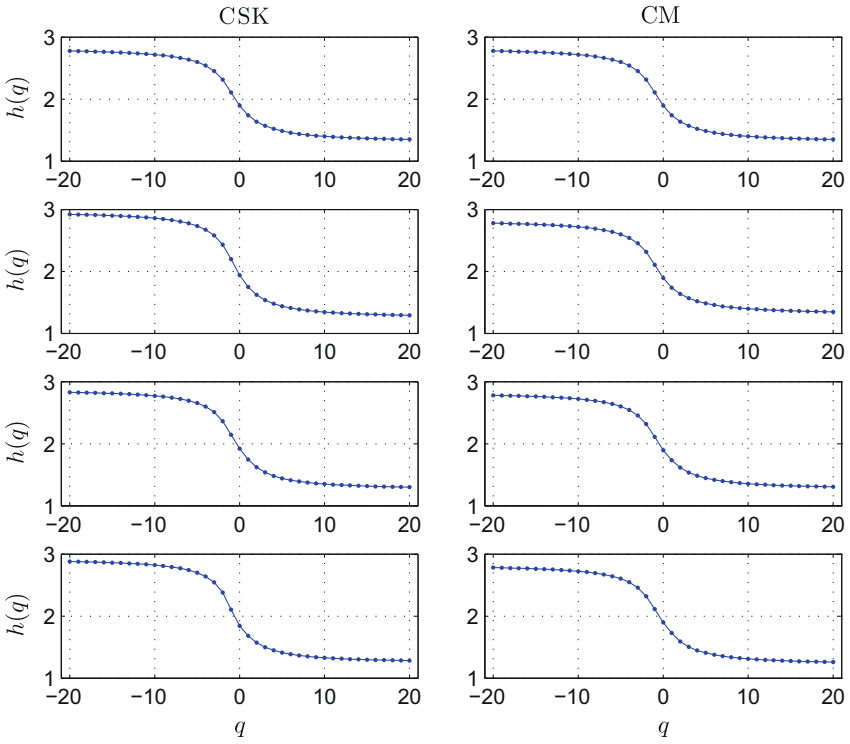

Fig. 1. Generalized Hurst exponent, $h(q)$, as a function of the order q for sampling period $\Omega_s = 1$ps and different message amplitude percent (0%, 2%, 10%, and 20% from top to bottom). Left and right columns correspond to the chaos shift keying (CSK) and chaos modulation (CM) encryption schemes, respectively.

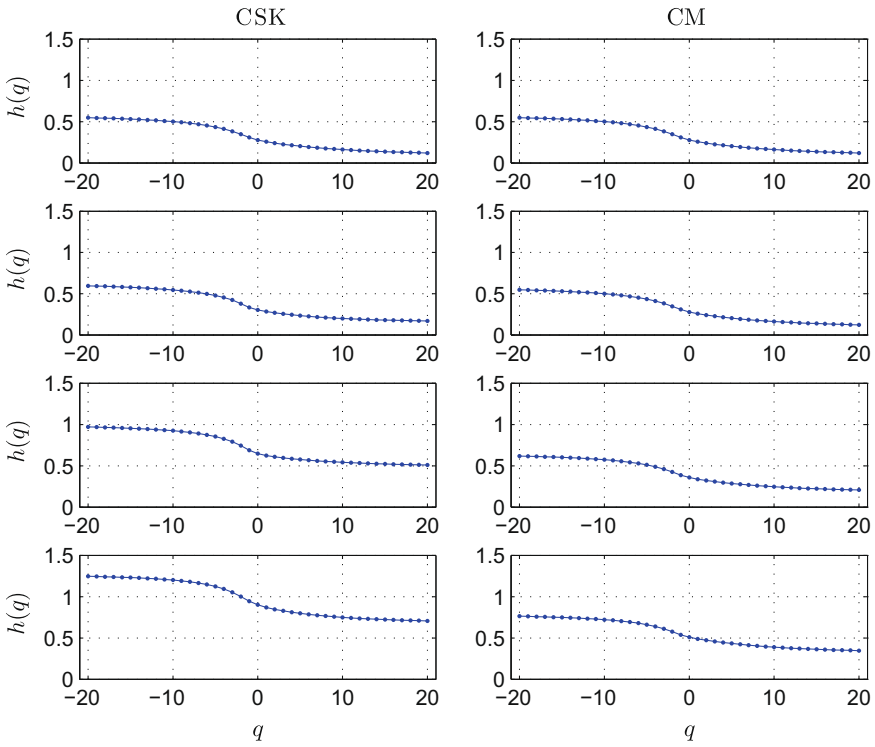

Fig. 2. Same as Fig. 1 for $\Omega_s = 10$ ps.

is the length of the time series. A similar q-range was chosen for the multifractal analysis of geoelectrical data [15], music frequency series [19] and color series of paintings [23]. Moreover, the s-range was selected according to the suggestions of Kantelhardt et al. [14].

Figs. 1–3 display the generalized Hurst exponents $h(q)$ for sampling periods $\Omega_s = 1$ ps, $\Omega_s = 10$ ps and $\Omega_s = 100$ ps, respectively. The results obtained for the two encryption schemes and for the different message amplitudes under analysis ca be compared. Only

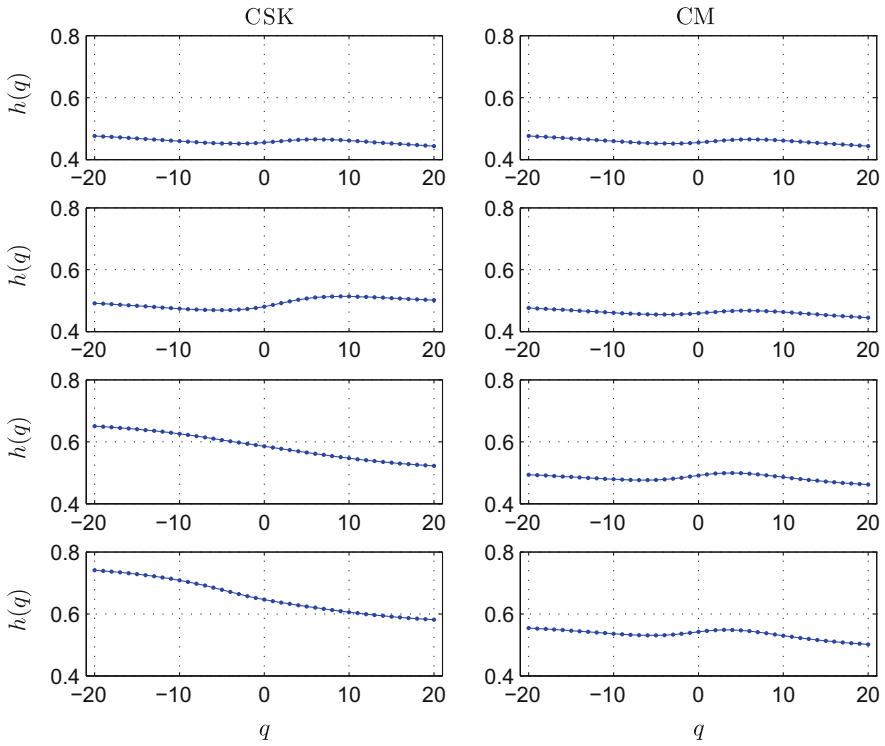

Fig. 3. Same as Fig. 1 for $\Omega_s = 100$ ps.

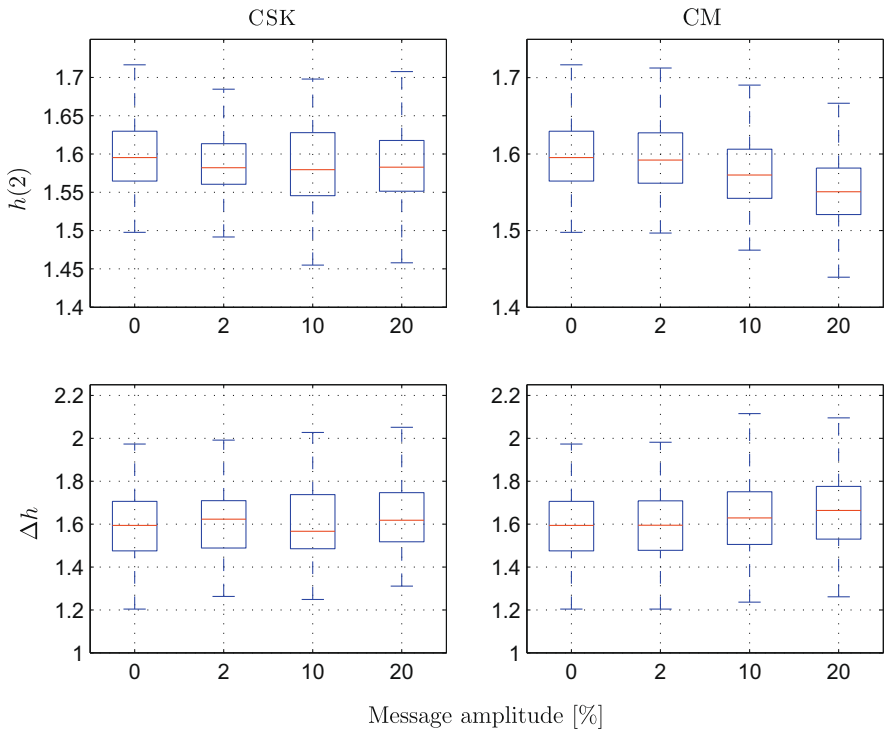

Fig. 4. Hurst exponent, $h(2)$, and multifractality degree, Δh, boxplots for sampling period $\Omega_s = 1$ ps and different message amplitude percent. Left and right columns correspond to the chaos shift keying (CSK) and chaos modulation (CM) encryption schemes, respectively.

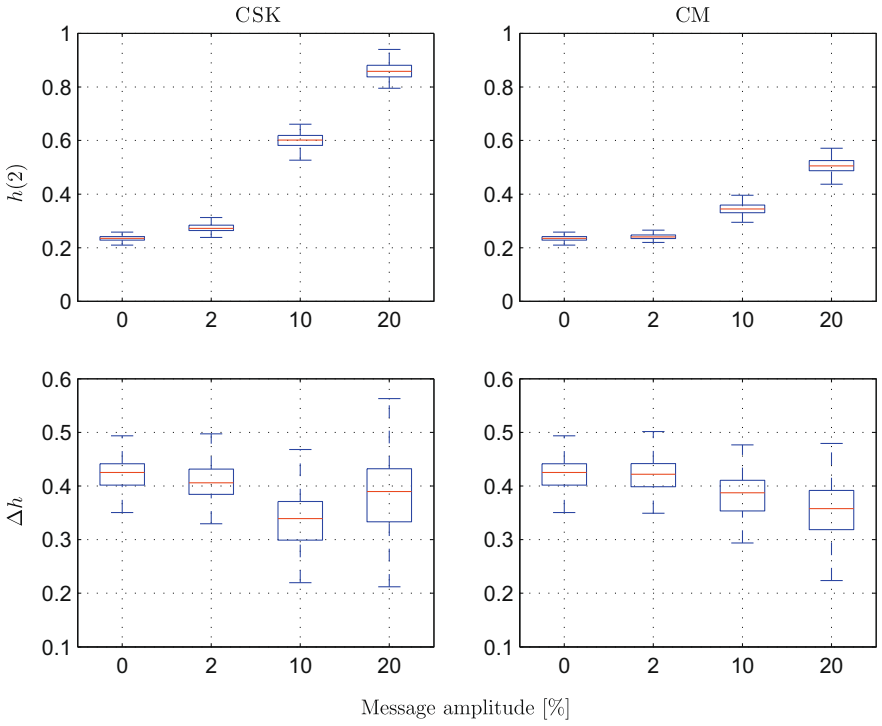

Fig. 5. Same as Fig. 4 for $\Omega_s = 10$ ps.

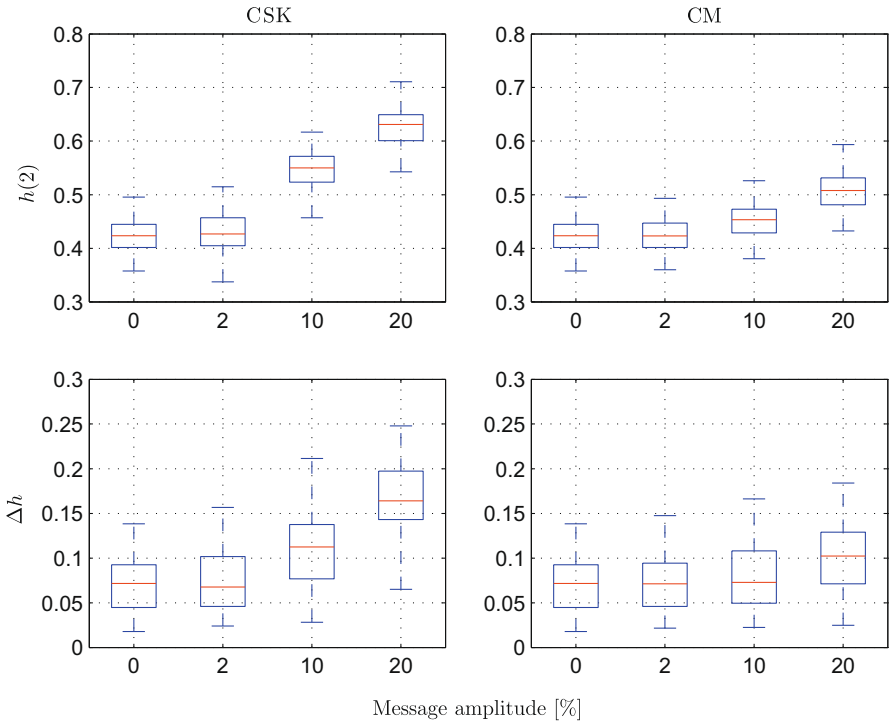

Fig. 6. Same as Fig. 4 for $\Omega_s = 100$ ps.

one realization, of the one hundred that we have considered, is shown. Note that for sampling period $\Omega_s = 1$ ps (Fig. 1) the generalized Hurst exponent curves are very similar for the different configurations of scheme and message amplitude. On the other hand, for sampling periods $\Omega_s = 10$ ps and $\Omega_s = 100$ ps (Figs. 2 and 3, respectively) important differences can be seen. Moreover, as the message amplitude increases, these differences also increase.

In order to visualize the results obtained for the different groups of data, boxplots[2] for our two quantifiers, the Hurst exponent and the multifractality degree, are shown in Figs. 4–6. These figures correspond to the three sampling periods $\Omega_s = 1$ ps, $\Omega_s = 10$ ps and $\Omega_s = 100$ ps, respectively. Comparing the estimated values for our two quantifiers we can analyze the effect that the different message amplitudes have on both encryption schemes.

It is clear that the results obtained depend on the temporal resolution at which the signals are sampled. For $\Omega_s = 1$ ps (Fig. 4) our two quantifiers yield very similar results for both encoding techniques and for the different message amplitudes. So, under this circumstance, they are useless to detect and quantify the effect of a message encoded within a chaotic carrier. The same result was recently found by Rosso et al. [35]. We attribute this behavior to an oversampling of the dynamics of the simulated time series. For $\Omega_s = 10$ ps (Fig. 5) the Hurst exponent allows a clear discrimination of the signals with message amplitudes of $A = 10\%$ and $A = 20\%$ when compared to pure chaotic carriers ($A = 0\%$) for both encryption schemes. There is a systematic increment of this quantifier while increasing the message amplitude. It is important to note that this effect is more pronounced for the CSK encryption scheme. The multifractality degree, on the other hand, does not vary appreciably for this sampling period. Finally, for $\Omega_s = 100$ ps both quantifiers increase as the message amplitude increases. However, in this case, the Hurst exponent tendency is less noticeable. Again we conclude that this discriminatory effect is stronger for the CSK encoding technique.

It should be stressed that in the CSK case the Hurst exponent shows a marked increment from an anti-persistent to a persistent behavior. In the CM analysis, however, this parameter lies always in the anti-persistent region. We guess that the larger message amplitudes introduce important correlations in the system dynamic increasing its predictability.

In summary, we have found that the Hurst exponent is better to discriminate the presence of an encoded message for a sampling period of $\Omega_s = 10$ ps while the multifractality degree is more sensitive for $\Omega_s = 100$ ps. With respect to the optimal message amplitude we have found that for $A = 2\%$ both multifractal quantifiers are unable to recognize the presence of a hidden message within the chaotic carrier. This value gives an estimation for the maximum amplitude for which the message cannot be detected. Finally, it is confirmed that the performance of the CM as encryption technique is better than the CSK.

5. Conclusions

We have shown that the multifractal indicators are powerful tools for quantifying the efficiency of encryption schemes. Under some circumstances, the proposed measures are useful approaches to distinguish the presence of a hidden message within a chaotic carrier. Particularly, the Hurst exponent seems to be a powerful tool for detecting and quantifying the presence of this hidden message. It allows a very clear discrimination of the signals with message amplitudes of the order of 5–10% or larger when compared to pure chaotic carriers (A=0%). From the multifractal approach we have shown that the chaos modulation encoding technique is better that the chaos shift keying. For the same amplitude, messages encoded with the former technique are more difficult to detect. These are relevant conclusions for secure optical communications based on chaos encryption.

The multifractal approch appears to be a more suitable and versatile way of assessing the security efficiency of encryption schemes for chaotic optical communication. Further research will be carried out to analyze the quality of other proposed encryption techniques such as OOPSK (On/Off Phase Shift Keying), where the feedback phase of the laser that generates the chaotic carrier is modulated [51]. Also the influence of the injection current, the length of the external cavity and the message modulation bit rate on the encryption performance will be analyzed. Finally, chaotic optical communication data experimentally obtained will be analyzed in the future with the tools introduced in this work in order to confirm our numerical results under real-world situations.

[2] This is a simple and powerful tool of graphically depicting groups of numerical data without making any assumptions of the underlying statistical distribution [49,50]. Boxplots 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.

Acknowledgements

The authors would like to thank an anonymous reviewer for his helpful comments. Luciano Zunino, Alejandra Figliola and Osvaldo A. Rosso were supported by Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina. The work of Miguel C. Soriano was supported by MEC (Spain) under a "Juan de la Cierva" contract. Darío G. Pérez was supported by Comisión Nacional de Investigación Científica y Tecnológica (CONICYT, FONDECYT Project No. 11060512), Chile, and partially by Pontificia Universidad Católica de Valparaíso (PUCV, Project No. 123.788/2007), Chile. Part of this work was supported by MEC (Spain) and Feder under Projects TEC-2006-28105-E and FIS2007-60327 (FISICOS), and by the EC Project PICASSO, IST-2005-34551. Osvaldo A. Rosso gratefully acknowledges support from Australian Research Council (ARC) Centre of Excellence in Bioinformatics, Australia.

References

[1] Y. Wang, G. Zhang, A. Wang, Opt. Commun. 277 (2007) 156.
[2] A. Bogris, K.E. Chlouverakis, A. Argyris, D. Syvridis, Opt. Lett. 32 (2007) 2134.
[3] Y. Li, Y. Wang, A. Wang, Opt. Commun. 281 (2008) 2656.
[4] V. Tronciu, I. Ermakov, P. Colet, C.R. Mirasso, Opt. Commun. 281 (2008) 4747.
[5] E. Rueda, C.A. Vera, B. Rodríguez, R. Torroba, Opt. Commun. 281 (2008) 5750.
[6] G.-Q. Xia, Z.-M. Wu, J.-F. Liao, Opt. Commun. 282 (2009) 1009.
[7] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcfa-Ojalvo, C.R. Mirasso, L. Pesquera, K.A. Shore, Nature 438 (2005) 343.
[8] M.C. Soriano, P. Colet, C.R. Mirasso, IEEE Photon. Technol. Lett. 21 (2009) 426.
[9] S. Donati, C.R. Mirasso (Eds.), Feature section on optical chaos and applications to cryptography, IEEE J. Quantum Electron. 38 (2002) 1138.
[10] L. Larger, J.P. Goedgebuer (Eds.), Cryptography using optical chaos, C.R. Phys. 5 (2004) 609.
[11] A. Uchida, F. Rogister, J. García-Ojalvo, R. Roy, Prog. Optics 48 (2005) 203.
[12] R. Lang, K. Kobayashi, IEEE J. Quantum Electron. 16 (1980) 347.
[13] A. Castro e Silva, J.G. Moreira, Physica A 235 (1997) 327.
[14] J.W. Kantelhardt, S.A. Zschiegner, E. Koscielny-Bunde, S. Havlin, A. Bunde, H.E. Stanley, Physica A 316 (2002) 87.
[15] L. Telesca, G. Colangelo, V. Lapenna, M. Macchiato, Phys. Lett. A 332 (2004) 398.
[16] N.K. Vitanov, E.D. Yankulova, Chaos, Solitons Fract. 28 (2006) 768.
[17] M.S. Movahed, G.R. Jafari, F. Ghasemi, S. Rahvar, M. Reza Rahimi Tabar, J. Stat. Mech. (2006) P02003.
[18] R. Barille, P. LaPenna, Appl. Opt. 45 (2006) 3331.
[19] G.R. Jafari, P. Pedram, L. Hedayatifar, J. Stat. Mech. (2007) P04012.
[20] A. Figliola, E. Serrano, O.A. Rosso, Eur. Phys. J. Special Topics 143 (2007) 117.
[21] G. Lin, Z. Fu, Physica A 387 (2008) 573.
[22] P. Shang, Y. Lu, S. Kamae, Chaos, Solitons Fract. 36 (2008) 82.
[23] P. Pedram, G.R. Jafari, Int. J. Mod. Phys. C 19 (2008) 855.
[24] S. Kumar, N. Deo, Physica A 388 (2009) 1593.
[25] Q. Zhang, C.-Y. Xu, Z. Yu, C.-L. Liu, Y.D. Chen, Physica A 388 (2009) 927.
[26] L.B.M. Silva, M.V.D. Vermelho, M.L. Lyra, G.M. Viswanathan, Chaos, Solitons Fract. 41 (2009) 2806.
[27] J. Wang, X. Ning, Y. Chen, Physica A 323 (2003) 561.
[28] A. Federico, G.H. Kaufmann, Appl. Opt. 46 (2007) 1979.
[29] A.K. Sen, Solar Phys. 241 (2007) 67.
[30] G. Wang, H. Huang, H. Xie, Z. Wang, X. Hu, Med. Eng. Phys. 29 (2007) 375.
[31] X. Yang, X. Ning, J. Wang, Physica A 384 (2007) 413.
[32] A.K. Sen, G. Litak, T. Kaminski, M. Wendeker, Chaos 18 (2008) 033115.
[33] C. Rodrigues Neto, Z.O. Guimarães-Filho, I.L. Caldas, I.C. Nascimento, Y.K. Kuznetsov, Phys. Plasmas 15 (2008) 082311.

[34] L. Zunino, B.M. Tabak, A. Figliola, D.G. Pérez, M. Garavaglia, O.A. Rosso, Physica A 387 (2008) 6558.
[35] O.A. Rosso, R. Vicente, C.R. Mirasso, Phys. Lett. A 372 (2007) 1018.
[36] J. Feder, Fractals, Plenum Press, New York, 1988.
[37] J.F. Muzy, E. Bacry, A. Arneodo, Phys. Rev. Lett. 67 (1991) 3515.
[38] C.-K. Peng, S.V. Buldyrev, S. Havlin, M. Simons, H.E. Stanley, A.L. Goldberger, Phys. Rev. E 49 (1994) 1685.
[39] P. Oświęcimka, J. Kwapień, S. Drożdż, Phys. Rev. E 74 (2006) 016103.
[40] H.E. Hurst, Trans. Am. Soc. Civ. Eng. 116 (1951) 770.
[41] B.B. Mandelbrot, J.W.V. Ness, SIAM Rev. 10 (1968) 422.
[42] A. Figliola, E. Serrano, G. Paccosi, M. Rosenblatt, Int. J. Bifurcat. Chaos (in press).
[43] K.E. Chlouverakis, A. Argyris, A. Bogris, D. Syvridis, Phys. Rev. E 78 (2008) 066215.
[44] W.-S. Lam, W. Ray, P.N. Guzdar, R. Roy, Phys. Rev. Lett. 94 (2005) 010602.
[45] R. Vicente, J. Daudén, P. Colet, R. Toral, IEEE J. Quantum Electron. 41 (2005) 541.
[46] V. Annovazzi-Lodi, M. Benedetti, S. Merlo, T. Perez, P. Colet, C.R. Mirasso, IEEE Photon. Technol. Lett. 19 (2007) 76.
[47] L. Ursini, M. Santagiustina, V. Annovazzi-Lodi, IEEE Photon. Technol. Lett. 20 (2008) 401.
[48] C.R. Mirasso, J. Mulet, C. Masoller, IEEE Photon. Technol. Lett. 14 (2002) 456.
[49] J.W. Tukey, Exploratory Data Analysis, Addison Wesley, 1977.
[50] Y. Benjamini, Am. Stat. 42 (1988) 257.
[51] M. Peil, T. Heil, I. Fischer, W. Elsäßer, Phys. Rev. Lett. 88 (2002) 174101.