

Chaos-Based Optical Communications: Encryption Versus Nonlinear Filtering

Adrian Jacobo, Miguel C. Soriano, Claudio R. Mirasso, and Pere Colet

Abstract—Several chaos encoding schemes codify the message in such a way that the mean value of the transmitted signal (carrier with the message) is different for bits “0” and “1”. We present a nonlinear filtering method that is able to detect very small changes in the mean value of a signal and therefore recover this kind of messages if its amplitude is larger than the chaotic fluctuations in the mean over the length of a bit. We also introduce a new codification method in which the mean value of the transmitted signal, over the length of each bit, is preserved and we show how it is able to beat the decryption scheme.

Index Terms—Chaos, dynamics, nonlinear optics, optical communications, semiconductor lasers.

I. INTRODUCTION

OPTICAL chaos-based communications have become popular in the past decade, evolving from a theoretical concept and an experimental demonstration [1] to an almost ready-to-use technique where successful field experiments have been reported [2]. Typically, the transmitted signal consists of a chaotic carrier generated by a semiconductor laser (SL) subject to feedback in which a message is encrypted. Then, a system similar to the emitter is necessary at the authorized receiver side to recover the message. Privacy relies on the difficulty to recover the message without the appropriate receiver. This depends not only on how strong the chaos is but also on the codification method. One of the most popular methods to encode information is chaos modulation (CM) [1], [3], [4] in which the message is encoded as a (small) modulation of the amplitude of the chaotic carrier.

Eventual eavesdroppers can attack in different ways. The simplest one is just trying direct detection of the modulated carrier. This attack usually fails except for messages codified with an extremely large modulation amplitude. A more sophisticated situation is such that the eavesdropper has a system *similar* to the authorized receiver although he may not know the parameters in which it operates. In this case, the degradation of the synchronization as a function of parameter mismatch [5]–[8]

Manuscript received July 10, 2009; revised October 12, 2009. Current version published February 12, 2010. This work was supported by MEC (Spain) and Feder under Projects TEC2006-1009/MIC (PhoDECC), TEC-2006-28105-E, and FIS2007-60327 (FISICOS); from EC Project PICASSO Grant IST-2005-34551. The work of M. C. Soriano was supported by the MEC under a “Juan de la Cierva” contract.

The authors are with the IFISC (CSIC-UIB) Instituto de Física Interdisciplinar y Sistemas Complejos, Campus Universitat Illes Balears, E-07122 Palma de Mallorca, Spain (e-mail: jacobo@ifisc.uib-csic.es).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/JQE.2009.2037980

plays a critical role in determining how similar the eavesdropper system should be to succeed. Other possibilities include the reconstruction of the chaotic attractor using the chaotic time series. This is only practical in systems where the local dynamics is low dimensional [9], [10]. Finally, one can also use adaptive systems trained to synchronize to the chaotic carrier, such as, for example, neural networks [11].

In this work, we take a different approach exploiting eventual pitfalls in the codification technique. We do not attempt to match the receiver nor to reconstruct the chaotic carrier, rather we study the possibility of using a nonlinear filtering technique to break chaos encrypted messages in encoding schemes in which the mean value of the chaotic carrier is not preserved. The method that we apply to break the encryption is based in previous work on noise filtering and contrast enhancement by using nonlinear dynamics of extended systems [12] which can be used to detect sudden jumps that are masked by noise.

In Section II, we introduce the model of two SLs subject to feedback and the encoding scheme. Then, in Section III, we show how the messages encoded with this scheme can be recovered using a nonlinear filtering technique. Finally, we propose an alternative encryption method that requires a more sophisticated implementation but that avoids detection by the nonlinear filter.

II. CHAOS ENCODING

We model the dynamics of the SL subject to optical feedback in terms of the Lang–Kobayashi equations [4]. The equations for the slowly varying amplitude of the electric field $E(t)$ and the carrier number $N(t)$ (in single-mode operation and low to moderate feedback) are

$$\dot{E}_{M,R}(t) = \frac{(1+i\alpha)}{2} [G_{M,R}(t) - \gamma_p] E_{M,R}(t) + \gamma E_{M,R}(t - \tau) e^{-i\Phi} + \kappa_r E_T(t) \quad (1)$$

$$\dot{N}_{M,R}(t) = \frac{I}{e} - \frac{N_{M,R}(t)}{\tau_N} - G_{M,R}(t) P_{M,R}(t) \quad (2)$$

where subindex M (R) refers to the emitter (receiver) laser and T to the transmitted signal (carrier with embedded message). The gain $G_{M,R} = g(N_{M,R} - N_o)/(1 + s P_{M,R})$. The laser intensity is $P(t) = |E(t)|^2$. For simplicity, we have assumed identical internal laser parameters and operating conditions and neglected noise effects in the lasers. Parameter $\alpha = 5$ is the linewidth enhancement factor, $\gamma_p = 0.5 \text{ ps}^{-1}$ is the photon decay rate, $\tau_N = 2 \text{ ns}$ is the carrier lifetime, $g = 1.5 \cdot 10^{-8} \text{ ps}^{-1}$ is the differential gain coefficient, $N_o = 1.5 \cdot 10^8$ is the carrier number at transparency, $s = 5 \cdot 10^{-7}$ is the gain compression

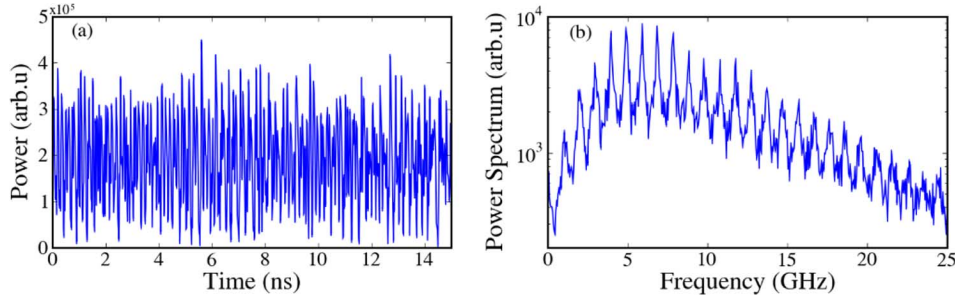


Fig. 1. (a) Time trace and (b) power spectrum of the chaotic carrier generated by a SL subject to feedback.

coefficient, $I = 2I_{th}$ is the injected current, $I_{th} = 14.7$ mA is the solitary laser threshold current, $\tau = 1$ ns is the feedback delay time, $\gamma = 25$ ns⁻¹ is the feedback strength, and $\Phi = 0$ is the optical feedback phase. The last term in (1) only appears in the equation for the receiver and it accounts for the injection of the emitter laser field into the receiver. Without loss of generality, we consider that this injection occurs instantaneously. An example of the generated chaotic carrier time trace and power spectrum is given in Fig. 1.

A high degree of synchronization between emitter and receiver is achieved by working in a closed loop configuration and for $\kappa_r > 60$ ns⁻¹ [6], [13].

We consider here a message encoded by modulating the emitter's chaotic carrier power

$$P_T(t) = (1 - \epsilon m(t))P_M(t) \quad (3)$$

where $P_T(t)$ is the transmitted signal, ϵ is the message modulation amplitude, $m(t)$ is the message being transmitted, taking values 0.5 and -0.5, and $P_M(t)$ is the chaotic carrier. The message can be recovered by the authorized receiver as

$$m'(t) = \frac{P_R(t) - P_T(t)}{\epsilon P_R(t)} \quad (4)$$

where $P_R(t)$ is the power emitted by the receiver laser. The recovery strongly depends on the quality of the synchronization between the emitter and receiver lasers. For $P_R(t) = P_M(t)$ (ideal synchronization) the message can be perfectly recovered. In practice one applies a Butterworth filter after detection to further clean the message, as it is typically done in all-optical chaos-based communications.

In some instances, it may not be straightforward to implement the division in (4), then the message is recovered by using

$$m''(t) = P_R(t) - P_T(t). \quad (5)$$

This is later filtered using a Butterworth filter and then normalized to the interval $[-1/2, 1/2]$. In this work, we will compare both decoding techniques with the eavesdropper attack introduced in Section III.

To illustrate the quality of the recovered messages, we show in Fig. 2 (a.1) a sample of a sequence of recovered bits using (4) and in Fig. 2 (a.2) the corresponding eye diagram of this sequence. Fig. 2 (b.1) and (b.2) show the time trace and eye

diagram of a sequence recovered using (5). To quantify the performance of the recovery process we use the quality factor

$$Q = \frac{\mu_1 - \mu_0}{\sigma_1 + \sigma_0} \quad (6)$$

where μ_1 and μ_0 are the average optical power of bits "1" and "0", and σ_1 and σ_0 are the corresponding standard deviations. A larger value of Q accounts for a better recovery of the message since the bit error rate is a monotonically decreasing function of Q [14]. For a 5-Gb/s message, the authorized receiver shows a clean and open eye diagram with $Q = 10.66$ in the case of $m'(t)$ and $Q = 4.78$ for $m''(t)$. Note that, by not making the division in (5), the quality factor is largely reduced, but message recovery is still possible.

One property of CM is that the mean value of the transmitted power during the length of a bit "1" ($\bar{P}_{T,1}$, where the bar stands for average over time) is different from a bit "0" ($\bar{P}_{T,0}$). This difference is

$$\bar{P}_{T,0} - \bar{P}_{T,1} = \epsilon \bar{P}_M. \quad (7)$$

This feature is shared by other encryption methods such as *chaos shift keying* [15] and *chaos masking* [4], [5], [16], which makes this discussion also relevant for these cases. If the message modulation amplitude ϵ is large, these differences on the mean value are easily detectable and the message can be recovered by using a linear filter, such as a low pass filter. One may also consider averaging the power over one bit. This requires the eavesdropper to know the exact bit rate as well as where the bit starts. As ϵ is reduced, usual filtering techniques fail to recover the message, nor does the average technique work. The use of a nonlinear filter can improve the ability to detect these deviations, and therefore push the range of secure operation to smaller amplitudes. The chaotic properties of the carrier set a limit for the message amplitudes that allow to operate in a secure regime. The average value of the chaotic carrier during a bit length fluctuates from one bit to another, and these fluctuations increase with the bit rate. We measure the standard deviation σ of these fluctuations and define Δ as the ratio between σ and the mean value of the chaotic carrier. For the chaotic carrier shown in Fig. 1(a), $\Delta = 0.02$ at 1 Gb/s, $\Delta = 0.05$ at 2.5 Gb/s, and $\Delta = 0.10$ at 5 Gb/s. Encoding a message with the CM method induces deviations from the mean value of the carrier. If these deviations are of the same order of magnitude or smaller than those of the chaotic signal, a filtering

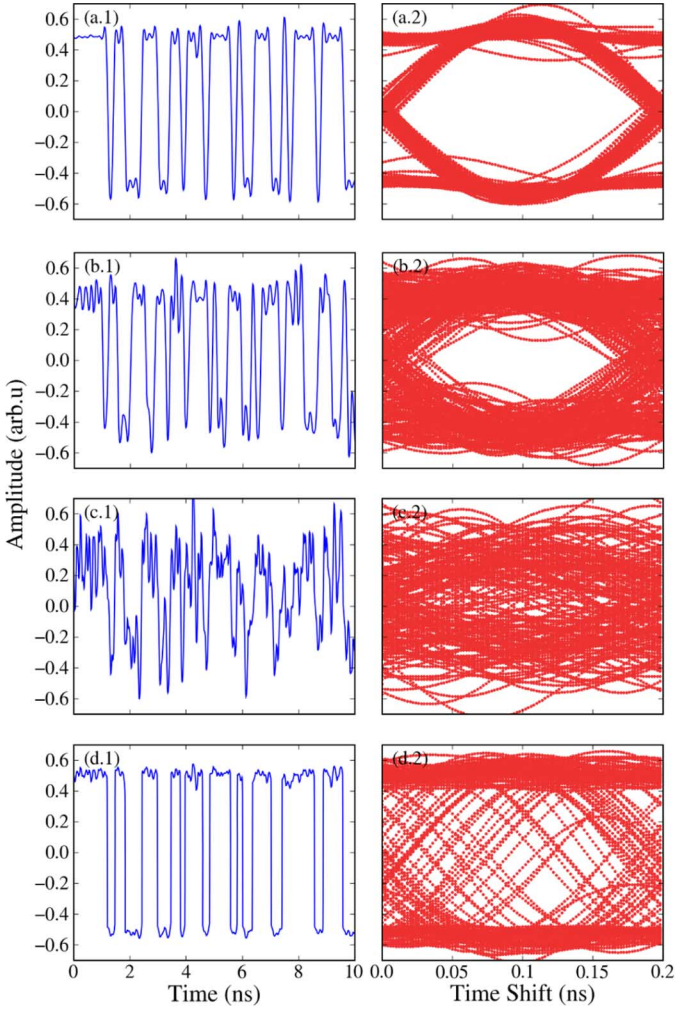


Fig. 2. Recovered messages (left) and eye diagrams (right) for 256 bits encoded with CM at 5 Gb/s ($\epsilon = 0.2$). (a) Authorized receiver $m'(t)$ ($\kappa_r = 75 \text{ ns}^{-1}$), (b) authorized receiver $m''(t)$, (c) GLE first pass ($a = 1000$, $r = 0.5$), and (d) GLE second pass ($a = 2$, $r = 0.65$).

technique will not be able to distinguish the intrinsic variations from the ones produced by the message, and therefore it will not be able to decrypt it. The drawback of working in this regime is that, to recover the message with enough quality, a very good synchronization between the emitter and the receiver is needed.

As we said, the variations of the chaotic signal at 5 Gb/s are about 10%, and we will show how, with a nonlinear filtering technique based on the forced Ginzburg Landau equation (GLE), we are able to decrypt signals up to these message modulation amplitudes, which is much better than what a linear filter can do.

III. BREAKING THE ENCRYPTION

To decrypt the message, we map the time series with the encoded message as the forcing of a nonlinear partial differential equation that presents a bistable steady state. The decoded message is recovered as the stationary state of the equation. We use the prototypical GLE [17] in one spatial dimension with a forcing term

$$\partial_t \psi(x, t) = a \cdot \partial_x^2 \psi(x, t) + \psi(x, t) - \psi(x, t)^3 + b \cdot h(x) \quad (8)$$

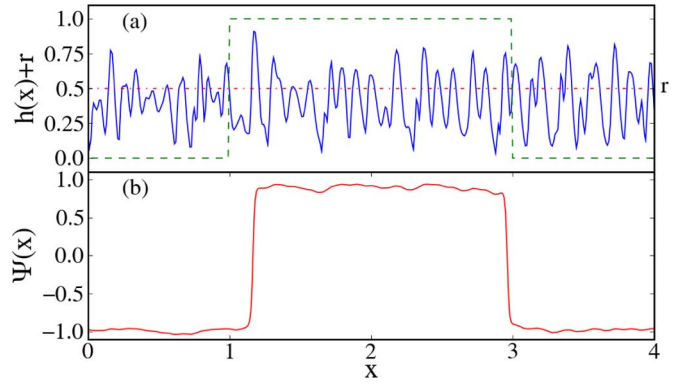


Fig. 3. Message recovery with the forced GLE. (a) The full line corresponds to the forcing term of (8) (chaotic carrier with the message) and the dashed line is the normalized encoded message. The dotted-dashed line corresponds to the reference level r . (b) Stationary state solution of (8) (recovered bits).

where ψ is the field, a is the diffusion constant, b is the forcing strength, and $h(x)$ is a space-dependent forcing. For convenience, we set $b = 1$.

Neglecting diffusion and $h(x)$, (8) has two stable stationary solutions, $\psi_+ = 1$ and $\psi_- = -1$ (plus an unstable solution at $\psi = 0$). Starting from $\psi(x, t = 0) = h(x)$, the points where $h(x) > 0$ will evolve to ψ_+ and those where $h(x) < 0$ will evolve to ψ_- . If we now consider the effect of diffusion, areas of a size of the diffusion length (given by $1/a$) that in average are larger than zero will approach to ψ_+ , and those areas that in average are lower than zero will approach to ψ_- as illustrated in Fig. 3. The diffusion will also wash out the fast frequencies of the chaotic signal. Finally, the effect of the forcing term $h(x)$ is to change the basin of attraction of ψ_+ and ψ_- , favoring the separation mechanism and balancing the effect of diffusion, making ψ follow the variations of $h(x)$. The GLE filtering method was initially intended to detect sudden jumps hidden by noise in ecological and biological experimental data¹ developing on prior ideas of using nonlinear extended systems to filter noise in images and selectively enhance the contrast [12], [18]. To apply the GLE filtering method to our case, we identify

$$h(x) = \frac{P_T(t)}{\text{MAX}(P_T(t))} - r \quad (9)$$

with $h(x)$, where r is a threshold parameter ($0 < r < 1$). Starting from $\psi(x, t = 0) = h(x)$, we let the equation evolve to the steady state, with a large value of a ($a = 1000$), this filters the fast frequencies of the chaos in a similar way that a low-pass filter would do. Once the field reaches the steady state, we set $a = 2$, with this value of the parameter the nonlinear mechanism comes into play enhancing the contrast of the signal from the reference level given by r , making the encoded message visible. The total effect of the process is to separate the zones (defined by the diffusion length) where the average of the signal is larger than r (i.e., “1” bits) and the zones where the average is less than r (i.e., “0” bits).

To illustrate the procedure, we start by processing the message using an encoding amplitude of $\epsilon = 0.2$. In Fig. 2 (c.1)

¹An implementation of the GLE method for filtering data series can be found online at <http://ifisc.uib-csic.es/users/jacobo/>

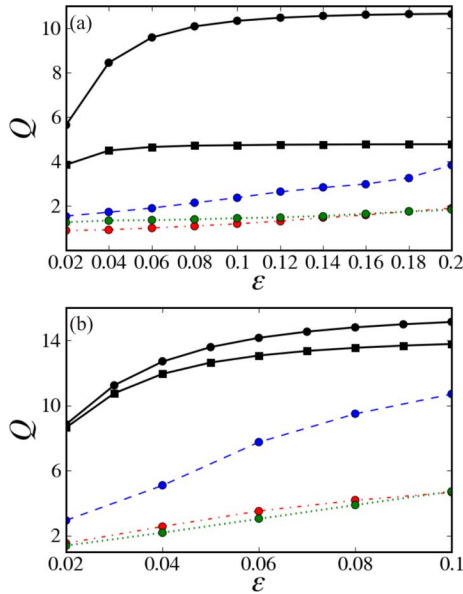


Fig. 4. Quality factor Q as a function of the message amplitude ϵ using CM at (a) 5 Gb/s and (b) 1 Gb/s. The solid lines correspond to the authorized receiver (circles for $m'(t)$ and squares for $m''(t)$), the dotted-dashed line (red online) to the GLE first pass and the dashed line (blue online) to the GLE second pass. The dotted line (green online) is the quality factor obtained by taking the mean value of the time series during the length of one bit.

and (c.2), we show a part of the time trace of the decoded message, and the eye diagram for the first pass with the filter, using $a = 1000$ and $r = 0.5$, respectively. It can be seen that, in this case, we are able to recover some features of the message but the eye diagram is very closed ($Q = 1.9$). This means that we would only be able to recover, at best, some bits. As previously said, this performance is similar to the one expected for a linear filter.

One should notice that the statistics of the message extracted by the GLE in the nonlinear filtering process may not be the same as for the authorized receiver. So the relationship between Q -factor and bit error rate may be different. Still the bit error rate will monotonically decrease function of Q , and therefore we will use it to characterize the accuracy of the recovered message. We choose to use the quality factor because it requires much less statistics and computation time than computing the bit error rate.

In Fig. 2 (d.1) and (d.2), we show the effect of a second pass using $a = 2$ and setting r to maximize the Q factor of the recovered message. Here, it can be seen that the message is nearly recovered (ten errors over 256 bits of the message), and the eye diagram is quite open ($Q = 3.85$). Considering these results, it would not be secure to encode messages with this amplitude using CM. In Fig. 4, we show the quality factor as a function of the message modulation amplitude ϵ . We can see that, applying the GLE twice, the results are much better than with a single pass with large diffusion (which is basically a linear filter). While the performance is not as good as the authorized receiver, it is still enough to decode the message if the value of ϵ is not too small. Performance decreases with decreasing ϵ . At 5 Gb/s [Fig. 4(a)], when ϵ approaches 0.1 (which is of the order of Δ), the nonlinear filtering method recovers only part of the message. However, it

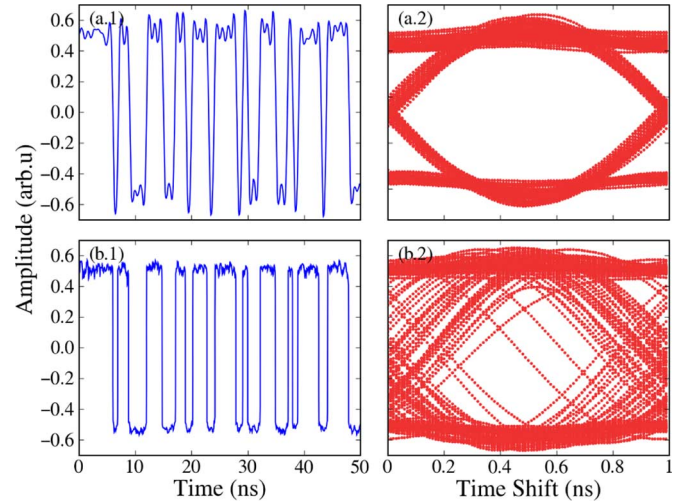


Fig. 5. Recovered messages (left) and eye diagrams (right) for 256 bits encoded with CM at 1 Gb/s ($\epsilon = 0.04$). (a) Authorized receiver $m''(t)$ ($k_r = 75 \text{ ns}^{-1}$). (b) GLE second pass ($a = 1$, $r = 0.65$).

should be kept in mind that reproducing part of the message is already a security threat.

Decreasing the bit rate the performance of the GLE filter improves. Fig. 5(a) shows the eye diagram for a message encoded at 1 Gb/s with $\epsilon = 0.04$ using CM and decoded by an authorized receiver using (5). Fig. 5(b) shows the message decoded by an eavesdropper using the GLE filter with $a = 1$ in the second pass. Fig. 4(b) shows the quality factor as function of the message amplitude ϵ at 1 Gb/s. Since for this bit rate Δ is smaller than for 5 Gb/s, the GLE filter provides a better performance for lower values of ϵ . In general, to prevent decoding using a nonlinear filter like the one considered here, the change in bit average power induced by message encoding should be of the order or smaller than the chaos fluctuations of the bit mean.

At this point, a few remarks on noise effects are in order since in practice the transmission scheme will always be subject to noise. As stated before, the GLE filtering method was initially designed to detect sudden jumps hidden by noise in data. As for the method, the chaotic carrier is considered as a kind of noise (whose origin is the deterministic chaos) that hides the message. If some amount of noise is added to the transmitted signal, within reasonable limits, the GLE will filter this noise along with the chaotic variations and the message will be recovered. The presence of noise in the system will also affect the ability of the authorized receiver to synchronize. The larger the noise, the worst the synchronization, requiring a larger message amplitude to keep the same quality factor at the authorized receiver. The larger the amplitude of the message, the better the performance of the GLE.

One can also compare the nonlinear method with the much simpler approach of taking the mean value of the time series during the length of one bit. In order to compute the mean value of one bit, we need to know both the transmission bit rate and the bit starting time. This is already one advantage of the GLE filtering method, for which this information is not needed (only the order of magnitude of the bit rate is needed, in order to adjust the value of a for the second pass). But the main advantage

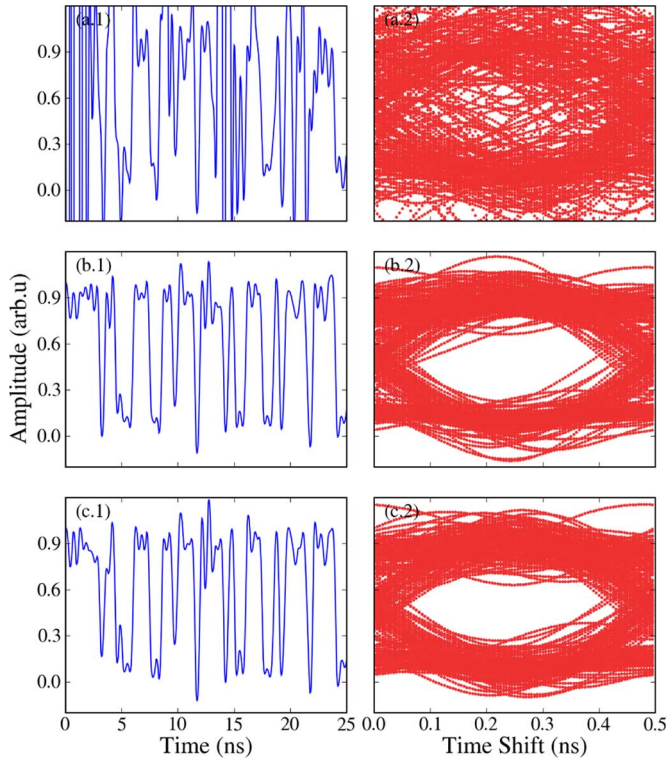


Fig. 6. Recovered messages (left) and eye diagrams (right) of 256 bits encoded with MPCM at 2 Gb/s for the authorized receiver ($\kappa_r = 75 \text{ ns}^{-1}$ and $\epsilon = 0.2$) with (a) $K = 0$, (b) $K = 0.05$, and (c) $K = 0.1$.

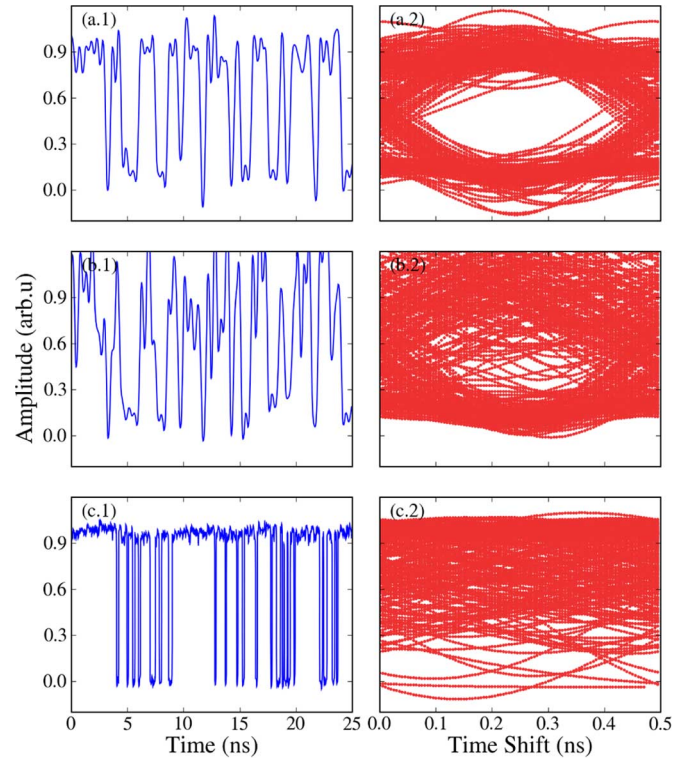


Fig. 7. Recovered messages (left) and eye diagrams (right) of 256 bits encoded with MPCM at 2 Gb/s ($\epsilon = 0.2$). (a) Authorized receiver $m'(t)$ ($\kappa_r = 75 \text{ ns}^{-1}$ and $K = 0.05$), (b) authorized receiver $m''(t)$, and (c) GLE second pass ($a = 1$ and $r = 0.65$).

of the nonlinear filtering can be seen in Fig. 4, where the dotted line shows the quality factor obtained by computing the average value over one bit. Here is clearly seen that due to its contrast enhancement capabilities the GLE filtering provides a much better quality factor than averaging over the bit length, and therefore the message can be decoded for smaller values of ϵ .

IV. NEW CODIFICATION SCHEME

The GLE filter acts by detecting changes in the mean value of the signal, therefore it is useless if the message is encoded in such a way that the mean value is the same for bits “1” and “0”. As an example of an encoding method which cannot be broken by the GLE filter, we introduce the mean preserving chaos modulation (MPCM) as

$$P_T(t) = (1 - \epsilon m(t))P_M(t) + \epsilon m(t)\bar{P}_M \quad (10)$$

where \bar{P}_M is the mean of the chaotic carrier and $m(t)$ is now a binary message taking values 0 and 1. This method, in which the message is encoded in the variations around the mean value, is an extension of CM in which the average power for bits one and zero is the same for any modulation amplitude, albeit more difficult to implement experimentally. As a possible implementation, one could consider dividing the output of the emitter in two beams. The power of one of the beams is modulated as $(1 - \epsilon m(t))P_M(t)$. The other beam goes through a low-pass frequency filter to obtain the power average which then is modulated as $\epsilon m(t)\bar{P}_M$. Finally, both beams are recombined.

The recovery of the message at the authorized receiver side needs to account for the mean of the transmitted signal

$$m'(t) = \frac{P_R(t) - P_T(t)}{\epsilon(P_R(t) - \bar{P}_M)}. \quad (11)$$

In order to recover the message with a good quality, the authorized receiver must neglect the data points in which the power of the receiver is close to the mean value \bar{P}_M . Specifically, we discard the data points that satisfy $|P_R(t)/\bar{P}_M - 1| < K$, where K is an arbitrary number larger than 0. Fig. 6 shows samples of the recovered message for different values of K and its corresponding eye diagrams for $\epsilon = 0.2$. In Fig. 6(a)–(c), the largest quality factor ($Q = 5.21$) is obtained for $K = 0.05$. In the latter case, 9% of the points are neglected. Notice that the neglected points do not imply the loss of bits in the message since the discarded portion of the time trace is much shorter than the length of one bit.

Fig. 7 (a.1) and (a.2) show the message recovered using (11) and the eye diagram for $\epsilon = 0.2$ and $K = 0.05$. The eye diagram shown in Fig. 7 (a.2) is clearly open. The eye diagrams have been obtained with the same synchronization degree between the emitter and receiver lasers than in the CM case ($\kappa_r = 75 \text{ ns}^{-1}$). The MPCM method enhances the security of the communications at the expense of sacrificing part of the quality of the recovered message. In Fig. 8, we show the quality factor of the recovered message by an authorized receiver for different values of ϵ . We can see that while the quality of the

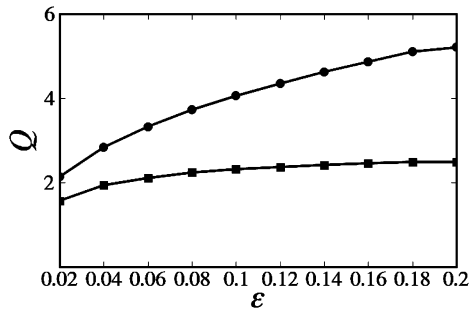


Fig. 8. Quality factor Q as a function of the encrypted message modulation amplitude ϵ using the mean-preserving chaos modulation (MPCM) scheme. The solid lines correspond to the authorized receiver (circles for $m'(t)$ and squares for $m''(t)$).

recovered message is lower compared to Fig. 4, even though we are modulating at a slower bit rate, the message is still well recovered.

As stated in Section II, the division in (11) may not be straightforward to implement experimentally, therefore we will also consider a second message recovery method, given by

$$m''(t) = |P_R(t) - P_T(t)|. \quad (12)$$

Fig. 7 (b.1) and (b.2) show the same message as Fig. 7 (a.1) and (a.2) but recovered using (12), when the division is not available. In this case, the eye diagram is barely open and the quality factor is reduced, as shown in Fig. 8. Given these results, it is not clear that this method could be implemented experimentally if the division is not feasible.

Now we apply the GLE method to a message encoded using this scheme. The result of the decoding operation is shown in Fig. 7(c) for $\epsilon = 0.2$. As can be seen, nothing can be recovered from the encoded message but random bits. Independently of the value of ϵ used to encode the message the GLE method is unable to extract it. Due to the way in which the GLE filter works in this case, it creates bits given by the variations of the chaotic signal only, and not by the variations in the mean value produced by the encoded message. We do not estimate the Q -factor since in this situation its value is basically meaningless.

V. CONCLUSION

In this work, we applied a nonlinear filtering method based on the GLE. Since this method is able to detect changes on the mean value of a data series, by properly tuning the parameters of the GLE, we were able to break communications schemes in which the change in bit average power induced by message encoding is larger than the one induced by the chaotic fluctuations. This nonlinear filtering method outperforms linear filters, due to the fact that besides filtering the fast frequencies of the chaotic signal as the linear filter does, the nonlinear one enhances the contrast of the bits “1” and “0”, improving the quality factor of the recovered message.

Therefore, if the codification is done without preserving the average power for bits “1” and “0”, the codification amplitude should be of the same order or smaller than the variations of the mean value of the chaotic signal over the length of one bit. Amplitude modulations larger than that pose a security threat since

the message could be eventually detected by an eavesdropper using the method proposed here or a similar one.

Finally, we have introduced a new codification method which, although its implementation is more cumbersome, constitutes an example of encoding that preserves the average power for bits “1” and “0”. In this way, the nonlinear filtering method described here or similar methods aiming at detecting variations in the mean become ineffective.

ACKNOWLEDGMENT

Discussions with Dr. V. Tronciu are acknowledged.

REFERENCES

- [1] G. D. VanWiggeren and R. Roy, “Optical communication with chaotic waveforms,” *Science*, vol. 279, pp. 1198–1200, 1998.
- [2] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, “Chaos-based communications at high bit rates using commercial fiber-optic links,” *Nature*, vol. 438, pp. 343–346, 2005.
- [3] A. Uchida, F. Rogister, J. Garcia-Ojalvo, and R. Roy, “Synchronization and communication with chaotic laser systems,” *Progress Opt.*, vol. 48, pp. 203–341, 2005.
- [4] C. Mirasso, P. Colet, and P. Garcia-Fernandez, “Synchronization of chaotic semiconductor lasers: Application to encoded communications,” *IEEE Photon. Technol. Lett.*, vol. 8, no. 2, pp. 299–301, Feb. 1996.
- [5] J. Ohtsubo, “Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback,” *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1141–1154, Sep. 2002.
- [6] R. Vicente, T. Pérez, and C. R. Mirasso, “Open versus closed loop performance of synchronized chaotic external-cavity semiconductor lasers,” *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1197–1204, Sep. 2002.
- [7] Y. C. Koumou, P. Colet, N. Gastaud, and L. Larger, “Effect of parameter mismatch on the synchronization of chaotic semiconductor lasers with electro-optical feedback,” *Phys. Rev. E*, vol. 69, pp. 056226-1–056226-15, 2004.
- [8] Y. C. Koumou, P. Colet, L. Larger, and N. Gastaud, “Mismatch-induced bit error rate in optical chaos communications using semiconductor lasers with electrooptical feedback,” *IEEE J. Quantum Electron.*, vol. 41, no. 2, pp. 156–163, Feb. 2005.
- [9] M. Itoh, C. W. Wu, and L. O. Chua, “Communication systems via chaotic signals from a reconstruction viewpoint,” *Int. J. Bifurcat. Chaos Appl. Sci. Eng.*, vol. 7, pp. 275–286, 1997.
- [10] C. Zhou and C. H. Lai, “Extracting messages masked by chaotic signals of time-delay systems,” *Phys. Rev. E*, vol. 60, pp. 320–323, 1999.
- [11] S. Ortin, J. M. Gutierrez, L. Pesquera, and H. Vasquez, “Nonlinear dynamics extraction for time-delay systems using modular neural networks synchronization and prediction,” *Phys. A, Statist. Mech. Appl.*, vol. 351, pp. 133–141, 2005.
- [12] A. Jacobo, P. Colet, P. Scotto, and M. San Miguel, “Use of nonlinear properties of intracavity type II second harmonic generation for image processing,” *Appl. Phys. B*, vol. 81, pp. 955–955, 2005.
- [13] M. C. Soriano, P. Colet, and C. R. Mirasso, “Security implications of open- and closed-loop receivers in all-optical chaos-based communications,” *IEEE Photon. Technol. Lett.*, vol. 21, no. 7, pp. 426–428, Apr. 2009.
- [14] A. Argyris, D. Kanakidis, A. Bogris, and D. Syvridis, “Experimental evaluation of an open-loop all-optical chaotic communication system,” *IEEE J. Sel. Topics Quantum Electron.*, vol. 10, no. 5, pp. 927–935, Sep.–Oct. 2004.
- [15] V. Annovazzi-Lodi, S. Donati, and A. Scire, “Synchronization of chaotic injected-laser systems and its application to optical cryptography,” *IEEE J. Quantum Electron.*, vol. 32, no. 6, pp. 953–959, Jun. 1996.
- [16] S. Sivaprakasam and K. A. Shore, “Signal masking for chaotic optical communication using external-cavity diode lasers,” *Opt. Lett.*, vol. 24, pp. 1200–1200, 1999.

- [17] D. Walgraef, *Spatio-Temporal Pattern Formation, With Examples in Physics, Chemistry and Materials Science*. New York: Springer-Verlag, 1996.
- [18] P. Scotto, P. Colet, and M. San Miguel, "All-optical image processing with cavity type-II second harmonic generation," *Opt. Lett.*, vol. 28, pp. 1695–1697, 2003.



Adrian Jacobo was born in Mar del Plata, Argentina, in 1980. He received the M.Sc. degree from the Universidad Nacional de Mar del Plata, Argentina, in 2003 and the Ph.D. degree in physics from the Universitat de les Illes Balears in 2009.

Since April 2009, he holds a postdoctoral contract at the Instituto de Física Interdisciplinar y Sistemas Complejos, Palma de Mallorca, Spain. His main research interest include nonlinear dynamics, spatiotemporal effects, and dynamics of localized structures.



Miguel C. Soriano was born in Benicarlo, Spain, in 1979. He received the Telecom Engineering degree from the Technical University of Catalonia, Spain, in 2002 and the Ph.D. degree in Engineering from the Free University of Brussels, Belgium, in 2006.

Since January 2008, he holds a "Juan de la Cierva" scientific contract at the Instituto de Física Interdisciplinar y Sistemas Complejos, Palma de Mallorca, Spain. His main research interests include nonlinear dynamics and synchronization properties of coupled semiconductor lasers.



Claudio R. Mirasso was born in Buenos Aires, Argentina, in 1960. He received the M.Sc. and Ph.D. degrees in physics from the Universidad Nacional de La Plata, Buenos Aires, Argentina, in 1984 and 1989, respectively.

After several Postdoctoral positions in Spain and the Netherlands, he became an Associate Professor with the Physics Department, Universiteit de les Illes Bolears (UIB), Palma de Mallorca, Spain, in 1996. He has authored or coauthored over 140 publications, including about 110 journal papers. His research interests include instabilities in semiconductor lasers, synchronization, and control of chaotic semiconductor lasers, dynamics and applications of delayed coupled semiconductor lasers, and applications of nonlinear dynamics.



Pere Colet was born in Vilafranca del Penedes, Barcelona, Spain, on April 21, 1964. He received the M.Sc. degree in physics from the Universitat de Barcelona, Spain, in 1987 and the Ph.D. degree in physics from the Universitat de les Illes Balears, Palma de Mallorca, Spain, in 1991.

In 1991, he became a Teaching Assistant at the Departament de Física, Universitat de les Illes Balears. From September 1991 to February 1993 and from April to September 1994, he was a Postdoctoral Fulbright Fellow at the School of Physics, Georgia Institute of Technology, Atlanta. In October 1994, he joined the Departament de Física, Universitat de les Illes Balears. Since May 1995, he has held a permanent research position at the Spanish Consejo Superior de Investigaciones Científicas. His present position is Reseach Professor at IFISC in Palma de Mallorca. He has coauthored over 90 papers in SCI journals as well as other 30 scientific publications. His research interests include fluctuations and nonlinear dynamics of semiconductor lasers, synchronization of chaotic lasers and encoded communications, synchronization of coupled nonlinear oscillators, pattern formation and quantum fluctuations in nonlinear optical cavities and dynamics of localized structures.