Communicating with Optical Hyperchaos: Information Encryption and Decryption in Delayed Nonlinear Feedback Systems

Vladimir S. Udaltsov, Jean-Pierre Goedgebuer, Laurent Larger, and William T. Rhodes
GTL-CNRS TELECOM, UMR CNRS 6603, Georgia Tech Lorraine, 57070 Metz, France
and Laboratoire d'Optique PM Duffieux, UMR 6603, Université de Franche-Comté, 25030 Besançon Cedex, France
(Received 24 May 2000; revised manuscript received 29 September 2000)

Recent theoretical studies and experimental demonstrations have shown the possibility of using chaos for the encryption of message signals in communication systems. Chaos is generated by systems with delayed nonlinear feedback, which feature hyperchaotic (i.e., of high dimensionality) dynamics. The different ways for the injection of the information in the emitter and the process of the synchronization of the receiver are considered. The analysis of all the possibilities can be used to choose the correct topology of communication systems and, more generally, to explain the behavior of any chaotic systems ruled by nonlinear difference-differential equations.

DOI: 10.1103/PhysRevLett.86.1892 PACS numbers: 05.45.Vx, 05.45.Jn, 42.65.Sf

Current methods for communicating message signals on noiselike chaotic carriers rely on a few general approaches [1]: the first one, applying the idea of controlled chaos, was developed by Ott, Grebogi, and Yorke; the second one, developed by Pecora and Carroll and later by Cuomo and Oppenheim, is based on what has been called synchronized chaos. Information is transmitted by adding a small-amplitude message signal to a large chaotic carrier, the latter effectively hiding the former. The message is extracted at the receiver by subtracting the chaos created in the receiver from the transmitted chaos-plus-message signal. Most of the studies in that field were implemented in electronics [2]. The question of synchronization of chaos has also been studied in optics [3]. We have demonstrated cryptographic systems, based on chaotic devices with so-called delayed nonlinear feedback (DNLF), which feature a high robustness of the chaos synchronization and a very good performance in terms of stability and information recovery [4,5].

In discussions about such systems, challenging questions are frequently asked: "Is it still possible to synchronize the receiver when the amplitude of the message signal is high?" "Is it always possible to recover directly the message at the receiver without using some additional processing?" This Letter is intended to address such questions in a comprehensive way.

A delay feedback system representative of those of concern is shown in Fig. 1. The system consists of a source, a nonlinear element, a detector, a first-order low-pass filter with a time constant τ, and a feedback loop with a delay time T. Such a scheme is general and can be used in a number of areas in physics, electronics, mechanics, biology, etc., to describe any chaotic systems with a nonlinear delayed feedback. The dynamical state of such a circuit is governed by a well-known nonlinear difference-differential equation, which takes the general form

$$v(t) + \tau \frac{dv}{dt}(t) = \beta F\{f[v(t - T)]\}, \qquad (1)$$

where $v(t)$ represents the chaotic signal in the system, $F\{\cdot\}$ is a nonlinear function featuring at least one extremum, $f[\cdot]$ is associated with the source, and β is the bifurcation parameter. For example, for the system [4], $v(t)$ represents the chaotically oscillating wavelength $\lambda(t)$, $F\{\cdot\}$ is related to the nonlinear transmission curve of the wavelength filter formed by the birefringent crystal, $f[\cdot]$ is the wavelength tuning curve of the laser diode, and β is the gain of the photodetector. For the electronic system [5], $v(t)$ is the signal driving the voltage controlled oscillator, $f[\cdot]$ is its tuning curve, and $F\{\cdot\}$ is the frequency response of a set of three oscillating circuits. In lasers, $v(t)$ can be the emitted power, $F\{\cdot\}$ is related to nonlinearities in the amplification medium, τ is the relaxation time of atoms or molecules, and T corresponds to the delay introduced by multiple reflections in the cavity [3]. We now consider the different ways in which the information signal $s(t)$ can be injected into the transmitter. There are five possible points of injection, indicated in Fig. 1 by the Roman numerals I–V. The addition of $s(t)$ to the feedback loop signal at a given transmitter input point modifies Eq. (1) in

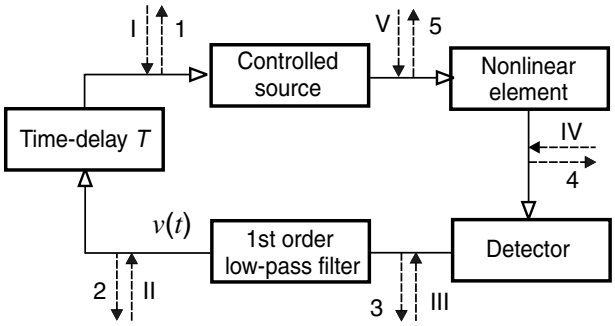

FIG. 1. Delayed-feedback nonlinear system for generation of chaos. Roman numerals designate points where a message signal can be injected into the system; arabic numerals designate points where the message-modulated chaotic signal can be tapped for transmission to the receiver system.

 0031-9007/01/86(9)/1892(4)$15.00

accordance with the following:

$$\text{I:}\quad v(t) + \tau \frac{dv}{dt}(t) = \beta F\{f[v(t-T) + s(t)]\}, \quad (2)$$

$$\text{II:}\quad v(t) + \tau \frac{dv}{dt}(t) = \beta F\{f[v(t-T) + s(t-T)]\}, \quad (3)$$

$$\text{III:}\quad v(t) + \tau \frac{dv}{dt}(t) = \beta F\{f[v(t-T)]\} + s(t), \quad (4)$$

$$\text{IV:}\quad v(t) + \tau \frac{dv}{dt}(t) = \beta F\{f[v(t-T)]\} + \beta s(t), \quad (5)$$

$$\text{V:}\quad v(t) + \tau \frac{dv}{dt}(t) = \beta F\{f[v(t-T)] + s(t)\}. \quad (6)$$

It can be seen from Eqs. (2)–(6) that, in each case, the information signal $s(t)$ changes the dynamics of the entire transmitter; thus the output signal represents more than simply the superposition of a chaotic signal and the information signal.

There are also five points in the feedback loop where the transmitter output can be obtained. These are indicated in Fig. 1 by Arabic numerals 1–5. The receiver consists of elements identical to those in the transmitter, and with the same topological layout. It is critical that the input to the receiver—the encrypted chaotic signal from the transmitter—passes through elements that are effectively identical to those in the transmitter and that are encountered in the same order. And the first element in the receiver must be the same as the element placed after the output point in the transmitter. Figure 2 illustrates the transmitter-receiver combination for case II/1. We consider this specific case for illustrating the synchronization and decoding process.

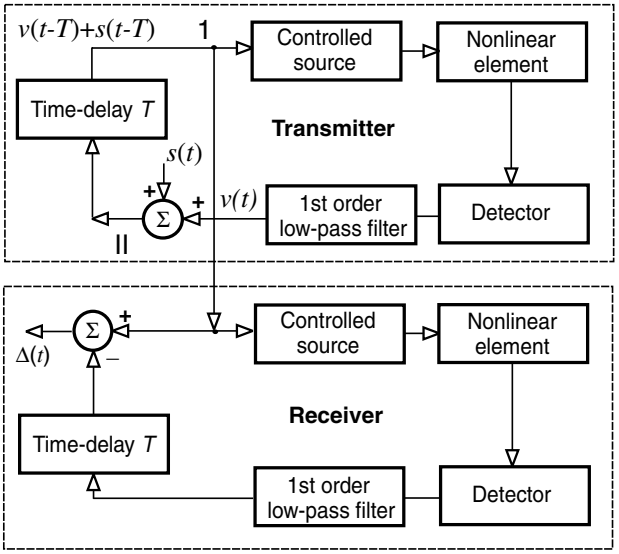

FIG. 2. Transmitter-receiver combination for case II/1. Message signal $s(t)$ is input to the transmitter loop. The output of the receiver, $\Delta(t)$, equals $s(t-T)$ if the receiver system is effectively identical to the transmitter.

The input to the receiver shown in Fig. 2 is given by $p(t) = v(t-T) + s(t-T)$. The difference-differential equation describing the chaos created in the receiver can be written in the form

$$v'(t) + \tau \frac{dv'}{dt}(t) = \beta F\{f[v(t-T) + s(t-T)]\}, \quad (7)$$

where $v'(t)$ is the chaos produced at the input of the time-delay element. Subtraction of Eq. (3) from Eq. (7) yields

$$v(t) + \tau \frac{dv}{dt}(t) - v'(t) - \tau \frac{dv'}{dt}(t) = 0, \quad (8)$$

a result that implies that $v'(t) - v(t) = 0$ asymptotically when $t \to \infty$, with time response τ. We thus conclude that the receiver synchronizes to the chaotic part of the signal $p(t)$ from the transmitter, independently of the message signal $s(t)$ [it must be noted that Eq. (8) is obtained for case II/1; it is not necessarily valid for the other cases]. Subtracting the chaos $v'(t-T)$ at the receiver-output from the receiver-input signal $p(t)$ yields the difference signal $\Delta(t) = p(t) - v'(t-T) = s(t-T)$. So, the system under consideration gives rigorously the original information signal $s(t)$, delayed by T. Recovery of the original message depends neither on the parameters of the chaotic carrier nor on the message signal. The method succeeds even if the amplitude of the message signal $s(t)$, its bandwidth, or both are larger than those of the chaotic carrier. In that latter case the information can be recovered without any degradation. That result is the answer to the first question asked earlier in this Letter.

The results of analysis for all possible cases are presented in Table I. The rigorous solutions $\Delta(t) = s(t)$ and $\Delta(t) = s(t-T)$, which yield an exact copy of the original message signal for any source and nonlinear element, are obtained only in seven cases, those cases that lie along the table diagonal and cases II/1 and IV/3.

Cases III/1, IV/1, III/2, and IV/2 yield difference signals $\Delta(t)$ ruled by differential equations (see Table I) whose solutions are of the form $\Delta(t) = \tau^{-1} \times [s(t) \star \exp(-t/\tau)]$, where $\star$ denotes a convolution. Those solutions are physically equivalent to filtering $s(t)$ by a low-pass filter with a cutoff frequency $(2\pi\tau)^{-1}$.

Cases I/5, II/5, III/5, and IV/5 require a specific post-processing, except if the f-function is a linear function of the form $f[v(t)] = \alpha v(t) + \omega$, where α and ω are constants. Cases I/5 and II/5 yield the full synchronization, and recovery of $s(t)$ is exact (see Table I). We put emphasis on that specific situation since it is usually met experimentally in optics and electronics. Cases III/5 and IV/5 are physically equivalent to filtering $s(t)$ by a low-pass filter.

The other ten cases do not allow the information to be extracted directly from the transmitted signal. The expression that governs the signal $\Delta(t)$ at the receiver output is

TABLE I. The difference signal $\Delta(t)$ for all possible cases of the information signal injection into the circuit and for all cases of the various output points.

Input point	Output point 1	2	3	4	5
I	$\Delta(t) = s(t)$	Processing	Processing	Processing	$\Delta(t) = \alpha\, s(t)$
II	$\Delta(t) = s(t - T)$	$\Delta(t) = s(t)$	Processing	Processing	$\Delta(t) = \alpha\, s(t - T)$
III	$\Delta(t) + \tau \frac{d\Delta}{dt}(t) = s(t - T)$	$\Delta(t) + \tau \frac{d\Delta}{dt}(t) = s(t)$	$\Delta(t) = s(t)$	Processing	$\Delta(t) + \tau \frac{d\Delta}{dt}(t) = \alpha\, s(t)$
IV	$\Delta(t) + \tau \frac{d\Delta}{dt}(t) = \beta\, s(t - T)$	$\Delta(t) + \tau \frac{d\Delta}{dt}(t) = \beta\, s(t)$	$\Delta(t) = \beta\, s(t)$	$\Delta(t) = s(t)$	$\Delta(t) + \tau \frac{d\Delta}{dt}(t) = \beta\alpha\, s(t)$
V	Processing	Processing	Processing	Processing	$\Delta(t) = s(t)$

given below, as an example, for case I/3:

$$\Delta(t) = \beta\, F\{f[v(t - T) + s(t)]\} - \beta\, F\{f[v(t - T)]\}, \tag{9}$$

In each case, if there is no message $s(t)$ at the transmitter input $[s(t) = 0]$, the receiver is synchronized to the transmitter. However, despite that synchronization, it is not possible to retrieve the message unless special postprocessing is employed. As an example of such postprocessing, consider case I/3 for the system [4]. The source in that system is characterized by a linear f-function, and the nonlinearity is given by $F(\lambda) = \sin^2(A\lambda + \Phi_0)$, where A and Φ_0 are parameters depending on the optical path-difference D of the birefringent wavelength filter, and on the center wavelength Λ_0 of the laser diode ($A = \frac{\pi D}{\Lambda_0^2}$ and $\Phi_0 = \frac{\pi D}{\Lambda_0}$). Solving Eq. (9) for that case yields the following expression for the message signal $s(t)$:

$$s(t) \propto \sin^{-1}\left\{\sqrt{\frac{\Delta(t)}{\beta} + \sin^2\{A[\lambda(t - T) + \Lambda_0]\}}\right\} - A[\lambda(t - T) + \Lambda_0], \tag{10}$$

where $\lambda(t - T)$ is the oscillating part of the wavelength of the signal generated by the laser diode in the receiver. Note that both $\Delta(t)$ and $\lambda(t - T)$ are required to calculate $s(t)$ using this equation. That obstacle makes processing hardly applicable in communications.

Consider now the case when the information signal is mixed with the chaotic signal outside the transmitter, as in the Pecora and Carroll method [1]. Analysis of the dynamics of the transmitter-receiver combination (for output 1 in Fig. 1) yields a difference signal $\Delta(t)$ at the receiver output governed by

$$\Delta(t) + \tau \frac{d[\Delta - s]}{dt}(t) = \beta\, F\{f[v(t - 2T)]\} - \beta\, F\{f[v(t - 2T) + s(t)]\}. \tag{11}$$

Recovery of the message signal $s(t)$ by means of Eq. (11) is at best not straightforward, and direct access to $s(t)$ is clearly impossible.

To verify the conclusions presented above we conducted experimental demonstrations, implementing the different configurations corresponding to Eqs. (2)–(6) for the transmitter along with the corresponding receiver equations. Experimental verifications were performed using the experimental device described earlier in this Letter [4]. Parameters of the experimental system were set as follows: $\Lambda_0 = 1550$ nm, $D = 11$ mm, $T = 500\ \mu$s, and $\tau = 9\ \mu$s. The value of the normalized bifurcation parameter β (see [4]) was equal to 22. The standard deviation of the chaotic fluctuations of the wavelength at about 1550 nm was 1 nm and the estimated dimension of the generated chaotic signal was $d \approx 500$. That value was obtained using the estimation $d \sim 0.4T/\tau$ calculated for a $\sin^2$-type nonlinearity in [6]. The information signal was a sine wave whose amplitude could be varied and whose frequency could be inside or outside the bandwidth of the chaos produced by the transmitter. An example of the chaotic carrier signal generated by the transmitter is shown in Fig. 3a. The difference signal $\Delta(t)$ obtained at the receiver output was obtained experimentally for the full-synchronization cases I/1, II/2, III/3, IV/4, V/5, II/1, and IV/3, where we have obtained the error-free signal extraction (example in Fig. 3b), and for cases I/5, II/5. We observed the low-pass filtering effect in the cases III/1, IV/1, III/2, IV/2, III/5, and IV/5.

The specific situation where postprocessing is required to recover the message from the difference signal $\Delta(t)$ was also tested for the cases I/2, I/3, I/4, II/3, II/4, and III/4 (see example I/3 in Fig. 3c). As a result of processing Eq. (10) we obtained the information signal $s(t)$ that is shown in Fig. 3d. The experimental verification of cases V/1, V/2, V/3, and V/4 could not be performed with the experimental setup, but all those cases were tested numerically using the Runge-Kutta procedure for solving the equations corresponding to the emitter and the receiver of the system [4]. We have investigated a wide range of values of the message-to-chaos ratio and observed that direct recovery of the message [analyzing the time series or the spectrum of the signal $\Delta(t)$] is then impossible. The case of mixing the message signal with the chaotic carrier outside the feedback loop also confirmed that the chaotic dynamics of the transmitter and receiver cannot be synchronized (Fig. 3e). The obtained experimental results agree completely with the analysis of the delayed-differential equations (Table I) that govern such chaotic systems. Performances in terms of signal-to-noise ratio are given in the captions of Fig. 3.

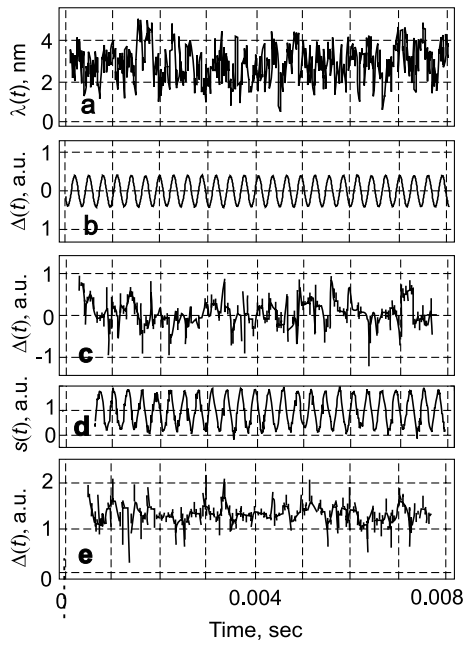

FIG. 3. Examples of signals produced experimentally. (a) Composite chaotic signal generated by the transmitter (II/1) formed by the addition of the message $s(t)$ with a message-to-chaos ratio of -20 dB; (b) the difference signal $\Delta(t)$ obtained for case II/1 (signal-to-noise ratio is measured to be -30 dB); (c) the difference signal $\Delta(t)$ for case I/3; (d) example of the processing Eq. (10) for case I/3; (e) receiver output $\Delta(t)$ corresponding to Eq. (11), when the message $s(t)$ is mixed with the chaotic carrier outside the transmitter with a -20 dB message-to-chaos ratio.

Thus the synchronization process in such systems is either fully insensitive or is highly sensitive to external perturbations, depending on the particular system configuration. In communications, all the cases yielding the rigorous recovery of the information, including the cases of a linear f-function, are equally acceptable for practical applications.

To conclude, the analysis of chaos synchronization presented in this Letter applies to any chaotic systems ruled by difference-differential equations. Returning to the questions raised earlier in the context of communication systems, we thus reach the following conclusion: The synchronization of DNLF systems and, hence, direct recovery of the message without postprocessing require that the signal input and transmitter output be assigned to suitable points in the transmitter. The synchronization process exhibited with the correct configurations is probably one of the most remarkable features of time-delayed feedback chaotic systems, which can produce high-dimensional chaos. We did not discuss the problem of security of DNLF systems (the reader is referred to [7]), reminding one that breaking systems with strong nonlinearities, i.e., described by a F function with multiple extrema [4,5], is still an open issue.

V. Udaltsov acknowledges the financial support of Centre National de la Recherche Scientifique (CNRS), France.

[1] E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990); L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990); K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[2] L. J. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992); T. Matsumoto, L. O. Chua, and K. Kobayashi, IEEE Trans. Circuits Syst. **33**, 1143 (1997); U. Parlitz, L. O. Chua, L. Kosarev, K. S. Halle, and A. Shang, Int. J. Bifurcation Chaos **2**, 973 (1992); M. Storace, Electron. Lett. **34**, 1077 (1998); M. Storace and F. Bizzarri, Electron. Lett. **35**, 1896 (1999).

[3] G. D. VanWiggeren and R. Roy, Science **279**, 1198 (1998); S. Sivaprakasam and K. A. Shore, Opt. Lett. **24**, 1200 (1999); S. Sivaprakasam and K. A. Shore, Opt. Lett. **24**, 466 (1999); H. D. I. Abarbanel and M. B. Kennel, Phys. Rev. Lett. **80**, 3153 (1998); C. R. Mirasso, P. Colet, and P. Garcia-Fernandez, IEEE Photonics Technol. Lett. **8**, 299 (1996); L. G. Luo, P. L. Chu, and H. F. Liu, IEEE Photonics Technol. Lett. **12**, 269 (2000).

[4] J. P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. Lett. **80**, 2249 (1998); J. P. Goedgebuer, L. Larger, H. Porte, and F. Delorme, Phys. Rev. E **57**, 2795 (1998); L. Larger, J. P. Goedgebuer, and J. M. Merolla, IEEE J. Quantum Electron. **34**, 594 (1998).

[5] L. Larger, V. S. Udaltsov, J. P. Goedgebuer, and W. T. Rhodes, Electron. Lett. **36**, 199 (2000).

[6] B. Dorizzi, B. Grammaticos, M. Le Berre, Y. Pomeau, E. Ressayre, and A. Tallet, Phys. Rev. A **35**, 328 (1987).

[7] K. M. Short and A. T. Parker, Phys. Rev. E **58**, 1159 (1998); J. B. Geddes, K. M. Short, and K. Black, Phys. Rev. Lett. **83**, 5389 (1999); Ch. Zhou and C.-H. Lai, Phys. Rev. E **60**, 320 (1999); C. Zhou and T. Chen, Phys. Lett. A **234**, 429 (1997).