Synchronization Scheme for Secured Communications System Based on Chaotic Signals

Paul E. Sterian

Research Center of Optical Engineering and Photonics, Politehnica University of Bucharest, Bucharest, Romania

In this work, a numerical investigation of a synchronization scheme for secure communication implemented with nonlinear optical ring cavities is performed. We have demonstrated that masking the information in a chaotic optical wave from a nonlinear ring cavity is technically feasible in a secured communication system. The synchronization is robust and analog information transmission is suitable for the specific case considered.

Keywords: deterministic chaotic system; synchronization; communication system
Received: 20 November 2009, **Revised**: 29 January 2010, **Accepted**: 5 February 2010

1. Introduction

Synchronization of periodic signals is a common phenomenon in many scientific areas. On the other hand, deterministic chaotic systems present the property of sensitivity with respect to initial conditions: two identical autonomous chaotic systems starting at very close initial conditions evolve so that the trajectories in the phase space start diverging exponentially and for large times they are uncorrelated. It seems that synchronization can not be reached in such systems. Nevertheless, it was recently proven [1] that certain chaotic systems may be linked such that their chaotic motions synchronize. The research in this direction is greatly motivated by the possibility of using chaotic signals as broadband carriers of analog and digital information [2-6]. Tests were performed using electronic circuits. For example, the message was added to a chaotic carrier signal and transmitted to a system which is a copy of that one creating the chaotic signal. The receiver synchronizes with the carrier signal and the message is recovered by a simple substraction of the receiver signal from the total transmitted one in an adequate electronic block.

It was a widespread idea that deterministic chaos will not have practical applications. The ability to design synchronizing chaotic systems may open opportunities for the use of chaotic signals in private communication, taking advantage of the unique features of chaotic signals. More than that, synchronization is structurally stable in this case and using chaotic signals may be preferable to periodic signals in certain cases where robustness is important.

2. Pecora-Caroll Synchronization Scheme

This is the most known method for synchronization subsystems [1]. An autonomous n-dimensional dynamical system given in the form of a flow:

$$\dot{\mathbf{u}} = \mathbf{f}(\mathbf{u}) \tag{1}$$

is decomposed into two subsystems,

$$\dot{\mathbf{v}} = \mathbf{f}_{\mathrm{v}}(\mathbf{v}, \mathbf{w}) \tag{2a}$$

$$\dot{\mathbf{w}} = \mathbf{f}_{\mathrm{w}}(\mathbf{v}, \mathbf{w}) \tag{2b}$$

with $\mathbf{v} = (u_1, ..., u_m)$, $\mathbf{w} = (u_{m+1}, ..., u_n)$ and $\mathbf{f} = (\mathbf{f}_{\mathrm{v}}, \mathbf{f}_{\mathrm{w}})$

Now create a new **w'** subsystem driven by the **v** subsystem:

$$\dot{\mathbf{w}}' = \mathbf{f}_{\mathrm{w}}(\mathbf{v}, \mathbf{w}') \tag{3}$$

i.e., given by the same vector field $\mathbf{f}_{\mathrm{w}}$. Subsystem **w'** synchronizes with subsystem **w**, i.e., $\|\mathbf{w}-\mathbf{w}'\| \to 0$ as $t \to \infty$ if the conditional Lyapunov exponents of subsystem **w** are all negative [1].

3. Proposed Communication System

A communication scheme compatible with the above synchronization method is presented in Fig. (1). In the transmission area, the subsystem **u** is called *master* system, while the **w** and **w'** subsystems are referred to as *slave* systems. Here, the link between the two subsystems in the transmission area is unidirectional. The encryption is done by using the chaotic signal of the slave system at the transmitter as carrier for

ISSN 1999-656X

the message. At the receiver, the slave system synchronizes with its replica at the transmitter through the one linking drive signal. This allows the extraction of the information from the total transmitted signal.

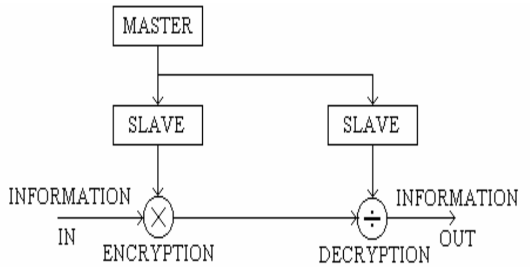

Fig. (1) Block scheme of a communication based on the synchronization of two chaotic systems

As optical fibers has already become a very important transmission medium and they have a great perspective, all-optical systems are advantageous compared to electrical ones. Taking this into account, the building blocks of the communication scheme in Fig. 1 are proposed ring optical cavities with a nonlinear optical medium inside (Fig. 2).

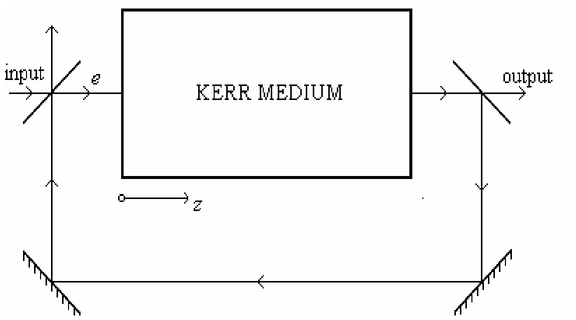

Fig. 2. Optical ring cavity configuration. The upper mirrors have reflectivities<1, whereas the lower ones are perfect reflectors

The nonlinear medium is a Kerr material whose response is described by the Debye relaxation equation. When the relaxation time constant of the medium is much longer than the delay time of the feedback of light and the medium is thin enough so that the phase shift of the electric field and the dissipation are small, the cavity is ruled by the set of ordinary differential equations [7]:

$$\dot{e} = a - be + i(\phi - \phi_0)e \qquad (4a)$$

$$\dot{\phi} = -\phi + |e|^2 \qquad (4b)$$

In the above, e is proportional to the slowly varying envelope of the electric field inside the cavity at z=0, ϕ is proportional to the phase shift of the electric field across the Kerr medium and time is expressed in Debye relaxation time units. a is a measure of the incident electric field amplitude, b characterizes the dissipation and ϕ_0 is the mistuning parameter of the cavity. See Ref. [7] for precise definitions. Equations (4) are valid when the ratio of the transit time of the cavity and the time relaxation constant of Kerr medium, denoted as $\rho\varepsilon$ (ρ=1/b), is $\rho\varepsilon$<<1, with ε<<1.

The output electric field of the cavity, which is proportional to e, exhibits not only bistability [8,9], but also a sequence of periodic and chaotic-like dynamics, as shown in Fig. (3) for the parameters b=0.2, ϕ=4 and a varying in both directions.

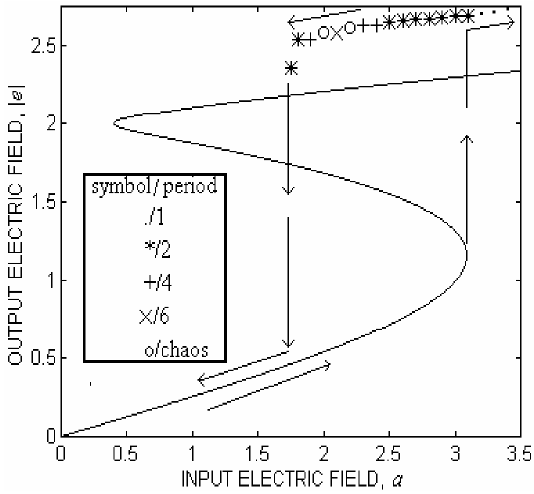

Fig. (3) Stationary states curve (solid curve) and actual dynamics (follow the arrows) of the optical cavity for b=0.2, ϕ_0=4, and *a* slowly sweeping in both directions. It can be seen that the system do not follow at all the upper branch of stationary states, but another one, composed of periodic orbits and chaotic ones. For the latter case, the temporal average of $|e|$ is plotted

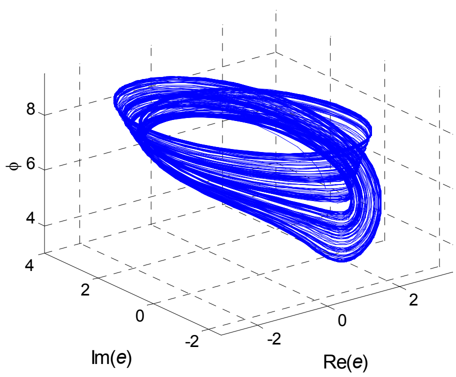

Fig. (4) Phase space representation of the chaotic dynamics of the optical cavity for *a*=2, *b*=0.2 and ϕ_0=4

We select the chaotic dynamics at a=2, completely establishing the master system at the transmitter. (Of course, an initial condition in the basin of attraction of the chaotic attractor is considered, not to get the other possible dynamics.) The chaotic attractor is presented in

Fig. (4). The dynamics is restricted to a quasi 2-dimensional manifold and it is interpreted as a result of the self-induced Rabi nutation of the electric field vector [7].

Below, the variables e and ϕ, as well as the parameters characterizing the master system will be written with the index 1. Indices 2 and 3 are reserved for the slave systems at the transmitter and receiver, respectively. Hence, the equations describing the communication scheme are:

$$\dot{e}_1 = a_1 - b_1 e_1 + \mathrm{i}(\phi_1 - \phi_{01})e_1 \quad (5a)$$

$$\dot{\phi}_1 = -\phi_1 + |e_1|^2 \quad (5b)$$

$$\dot{e}_2 = \exp(\rho\varepsilon\phi_1)c_{12}e_1 - b_2 e_2 + \mathrm{i}(\phi_2 - \phi_{02})e_2 \quad (5c)$$

$$\dot{\phi}_2 = -\phi_2 + |e_2|^2 \quad (5d)$$

$$\dot{e}_3 = \exp(\rho\varepsilon\phi_1)c_{13}e_1 - b_3 e_3 + \mathrm{i}(\phi_3 - \phi_{03})e_3 \quad (5e)$$

$$\dot{\phi}_3 = -\phi_3 + |e_3|^2 \quad (5f)$$

The coupling of cavities 1 and 2 and 1 and 3, respectively, is introduced through the complex quantities c_{12} and c_{13} that include both the attenuation and the phase shift of the signals during propagation between cavities. To be in agreement with Pecora and Caroll synchronization method, the two slave systems are characterized by identical parameters.

The choice b_2=b_3=0.2, ϕ_{02}=ϕ_{03}=4, c_{12}=c_{13}=0.2exp(0.2i) and $\rho\varepsilon$=0.01 gives synchronization as shown in Fig. (5). On the average, the synchronization errors decay exponentially.

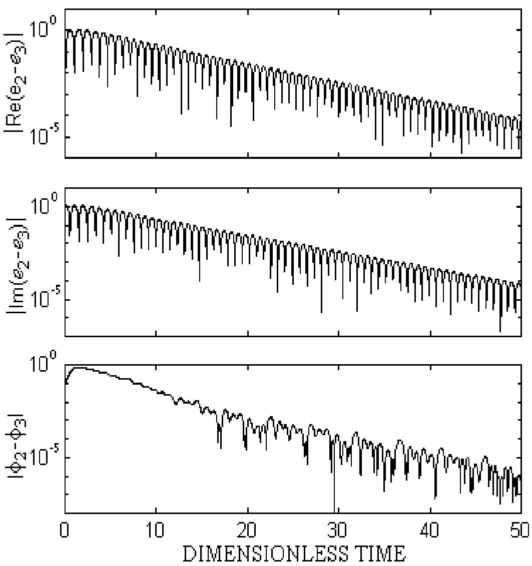

Fig. (5) Synchronization of optical cavities 2 and 3 both driven by the output signal from cavity 1. The values of the parameters are a_1=2, b_1=0.2, ϕ_{01}=4, $\rho\varepsilon$=0.01, b_2=b_3=0.2, ϕ_{02}=ϕ_{03}=4 and c_{12}=c_{13}=0.2exp(0.2i)

Numerical simulations prove that synchronization holds for any initial conditions and large ranges of parameter values. Besides, the synchronization is robust with respect to deviations from the identity of the slave systems up to about 10% in the parameter values. Parameters that may have significant different values are the coupling coefficients c_{12} and c_{13}. Figure (6) shows that synchronization errors stabilize at tiny values for c_{12} and c_{13} slightly different.

4. Discussion

A good encryption is enabled by a chaotic in a high degree of the carrier signal. This is given, for instance, by high values of the largest Lyapunov exponent and a high entropy [10]. Of special interest here is the mutual information of signal driving the slave system at transmitter and carrier signal. Taking the modulus of the electric field wave as signal, the plot $|e|_2$ versus $|e|_1$ is given in Fig. (7) and shows a small correlation of the two signals. The mutual information calculated based on the algorithm first proposed in Ref. [11] is about 2 bits, leading to a tough interception of the information.

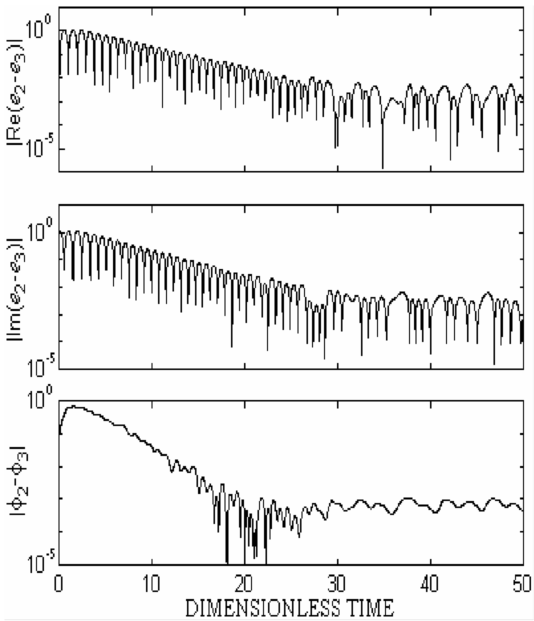

Fig. (6) Synchronization of optical cavities 2 and 3 when c_{13}=1.05c_{12}. All the other values of the parameters are as in Fig. (5)

The form of the carrier wave signal makes it suitable for an analog information signal. Frequency bandwidth of the carrier signal is about the reciprocal of time relaxation constant of Kerr medium. For instance, in case of carbon sulphide this quantity is of the order of 10^{12}Hz.

A specific model [Eqs. (4)] of the optical ring cavity has been investigated. For an improved modelling of the interaction processes in the system, see Refs. [12,13] for quantum formalisms of the interaction of an electromagnetical (optical) field with atomic media. Upper bound limit of transmission

ISSN 1999-656X

capacity is determined by quantum noise [14] establishing the theoretical limit of performances. Additional difficulties appear for the noise treatment in case of a carrier optical originating from a source with both optical and atomic coherence weights dependent on the operation conditions of the source.

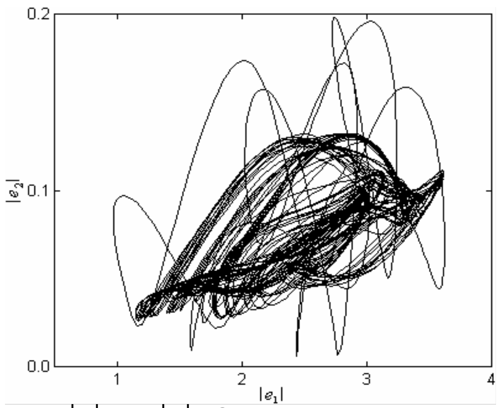

Fig. (7) $|e|_2$ vs. $|e|_1$. Same parameter values as in Fig. (5)

Masking digital information needs random sequences of pulses separated through large time intervals where the amplitude signal is very small. This kind of chaotic signals is available from other optical systems like semiconductor lasers with injection current modulation [15], where a modulation frequency in the GHz range ensures a good transmitting speed for the bits. A semiconductor laser with external cavity is expected to be used in information encoding at much higher bit rates.

5. Conclusion

In conclusion, we have demonstrated that masking the information in a chaotic optical wave from a nonlinear ring cavity is technically feasible in a secured communication system.

References

[1] L.M. Pecora and T.L. Caroll, *Phys. Rev. A* 44(4) (1991) 2374-2383.
[2] S. Hayes, C. Grebogy and E. Ott, *Phys. Rev. Lett.*, 70(20) (1993) 3031-3034.
[3] K.M. Cuomo and A.V. Oppenheim, *Phys. Rev. Lett.*, 71(1) (1993) 65-68.
[4] P. Colet and R. Roy, *Opt. Lett.*, 19(24) (1994) 2056-2058.
[5] U. Parlitz et al., *Phys. Rev. E*, 53(5) (1996) 4351-4361.
[6] P.M. Alsing et al., *Phys. Rev. E*, 56(6) (1997) 6302-6310.
[7] K. Ikeda and O. Akimoto, *Phys. Rev. Lett.*, 48(9) (1982) 617-620.
[8] I.M. Popescu, E. Stefanescu and P. Sterian, *Rev. Roum. Phys.*, 21(3) (1986) 221-235.
[9] P.E. Sterian, O. Rancu and I.M. Popescu, "Complex dynamics of radiation field in the transition area of optical bistability", in *Int. Conf. on Trends in Quantum Electronics, Proc. SPIE*, 1033 (1988) 154-157.
[10] G.L. Baker and J.P., Gollub, **"Chaotic Dynamics"**, Cambridge University Press, Cambridge (1990).
[11] A.M. Fraser and H.L. Swinney, *Phys. Rev. A*, 33(2) (1986) 1134-1140.
[12] P.E. Sterian, **"Fotonica"**, Bucuresti, Printech (2000).
[13] E. Stefanescu and P.E. Sterian, *Opt. Eng.*, 35(6) (1996) 153-155.
[14] P.E. Sterian, *Transmisia optica a informatiei*, Vol. I, II, Bucuresti, Editura Tehnica (1983).
[15] C.-H. Lee, T.-H. Yoon and S.Y. Shin, *Appl. Phys. Lett.*, 46(1) (1985) 95-97.