Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Communications in Nonlinear Science and Numerical Simulation 13 (2008) 645–659
Communications in Nonlinear Science and Numerical Simulation
www.elsevier.com/locate/cnsns

Communicating via synchronized time-delay Chua's circuits

C. Cruz-Hernández [a,*], N. Romero-Haros [b]

[a] CICESE, Telematics Direction, P.O. Box 434944, San Diego, CA 92143-4944, USA
[b] Electronics and Telecommunications Department, Scientific Research and Advanced Studies of Ensenada (CICESE), Km. 107 Carretera Tijuana-Ensenada, 22860 Ensenada, BC, Mexico

Received 9 March 2006; received in revised form 22 June 2006; accepted 22 June 2006
Available online 22 August 2006

Abstract

In this work, we apply the Generalized Hamiltonian forms and observer approach to synchronize time-delay-feedback Chua's circuits to transmit encrypted confidential information. We show by means of two communication schemes the quality of the recovered information, and at the same time, we have enhance the level of encryption security.

PACS: 05.45.Jn; 05.45.Xt; 05.45.Vx; 05.45.Gg; 89.75.−k

Keywords: Hyperchaos synchronization; Time-delay-feedback Chua's circuit; Observers; Secure communication

1. Introduction

Chaos synchronization has attracted much attention in recent years see e.g. [1–7] and references therein. This property is supposed to have interesting applications in different fields, particularly to design secure communication systems. Data encryption using chaotic dynamics was reported in the early 1990s as a new approach for encoding. Different techniques have been developed in order to hide information using chaos synchronization, such as *chaotic masking*, *chaotic switching*, and *chaotic parameter modulation*. However, it has been shown see e.g. [8] that encrypted signals by means of comparatively "simple" chaos with only one positive Lyapunov exponent does not ensure a sufficient level of security. For higher security, the hyperchaotic systems characterized by more than one positive Lyapunov exponent are advantageous over simple chaotic systems. Two factors of primordial importance in security considerations related to chaotic communication are: the dimensionality of the chaotic attractor, and the effort required to obtain the necessary parameters for the matching of a receiver dynamics.

On the basis of these considerations, one way to enhance the level of encryption security is by applying proper cryptographic techniques to the information in combination with chaos [9,10]. Another way is to encode information by using high dimensional chaotic attractors, or hyperchaotic attractors, which take

* Corresponding author. Tel.: +1 52 646 1750500/1736089; fax: +1 52 646 1750537.
E-mail address: ccruz@cicese.mx (C. Cruz-Hernández).

1007-5704/$ - see front matter
doi:10.1016/j.cnsns.2006.06.010

advantage of the increased randomness and unpredictably of the higher dimensional dynamics. In such option, one generally encounters *multiple positive Lyapunov exponents*. However, hyperchaos synchronization is a much more difficult problem (see e.g. [11–13], and for discrete-time context [14]). Most of the previous work done on hyperchaos synchronization has been concentrated on finite-dimensional systems described by ordinary differential equations. Thus, the number of positive Lyapunov exponents is limited by dimension of the state space.

As alternative way of constructing synchronized hyperchaotic systems can be based on delay differential equations, such systems have an infinite-dimensional state space and can produce hyperchaos with an arbitrarily large number of positive Lyapunov exponents. It has been known that even a very simple first-order oscillator with a time-delay can produce extremely complex hyperchaotic behaviors [15,16]. This property has stimulated the design of secure communication systems which claimed to have low detectability [17,18].

The objective of this work is to use the Generalized Hamiltonian forms and observer approach developed in [3] to synchronize time-delay-feedback Chua's circuits. Moreover, we apply this approach to transmit encrypted confidential information. A similar idea was used in [19] with the substantial differences: the modified communication scheme used here, is such that the encrypted information can be recovered faithfully, and effects of noise in channel are considered.

2. Review of synchronization via Generalized Hamiltonian systems and observer design

2.1. Hamiltonian systems

The Hamiltonian systems are the systems in the form of well-known Hamiltonian's canonical equations which represents physical systems. Recently, the Generalized Hamiltonian systems are introduced as generalization of Hamiltonian systems, which include many passive electric circuits and a class of nonholonomic systems. Moreover, this formulation is very tractable because it intrinsically contains the passivity property, which is widely exploited to solve several significant problems, as in this work, synchronization of chaotic systems.

Hamiltonian systems are a reformulation of Lagrangian mechanics, where the equations of *motion* are based on generalized coordinates (*generalized momenta*) q_j for $j = 1,\ldots,n$, and matching generalized velocities (*generalized coordinates*) $\dot{q}_j = \mathrm{d}q_j/\mathrm{d}t$ for $j = 1,\ldots,n$. Hamiltonian mechanics aims to replace the generalized velocity variables with generalized momentum variables, also known as *conjugate momenta*. By doing so, it is possible to handle certain systems, such as aspects of quantum mechanics that would otherwise be even more complicated. For each generalized velocity, there is one corresponding conjugate momentum, defined as $p_j = \partial L/\partial \dot{q}_j$ for $j = 1,\ldots,n$, where $L = L(q_j, \dot{q}_j, t)$ denotes the *Lagrangian function*, expressed in generalized momenta and generalized coordinates, and n is the number of degrees of freedom of the system. For example, in Cartesian coordinates, the generalized momenta are the physical linear momenta, in polar coordinates, the generalized momentum corresponding to the angular velocity is the physical angular momentum.

The *Hamiltonian function* is the *Legendre transform* of the Lagrangian function as follows:

$$H(q_j, p_j, t) = \sum_{j=1}^{n} \dot{q}_j p_j - L(q_j, \dot{q}_j, t). \tag{1}$$

In general, the Hamiltonian is a function of the generalized coordinates, of the generalized momenta, and of the time t, $H = H(q_j, p_j, t)$. If the transformation defining the generalized coordinates are independent of t, in many physical situations, can be shown that H is equal to the total energy of the system, i.e. $H = T + V$ where T is the *kinetic energy* and V is the *potential energy*. Taking the differential of (1), we have

$$\begin{aligned} \mathrm{d}H(q_j, p_j, t) &= \sum_{j=1}^{n} \left[\left(\frac{\partial H}{\partial q_j} \right) \mathrm{d}q_j + \left(\frac{\partial H}{\partial p_j} \right) \mathrm{d}p_j \right] + \left(\frac{\partial H}{\partial t} \right) \mathrm{d}t \\ &= \sum_{j=1}^{n} \left[\dot{q}_j \, \mathrm{d}p_j + p_j \, \mathrm{d}\dot{q}_j - \left(\frac{\partial L}{\partial q_j} \right) \mathrm{d}q_j - \left(\frac{\partial L}{\partial q_j} \right) \mathrm{d}\dot{q}_j \right] - \left(\frac{\partial L}{\partial t} \right) \mathrm{d}t. \end{aligned}$$