Available online at www.sciencedirect.com

ScienceDirect

Mathematics and Computers in Simulation 112 (2015) 14–27

MATHEMATICS AND COMPUTERS IN SIMULATION

www.elsevier.com/locate/matcom

Original articles

Performance improvement of chaotic encryption via energy and frequency location criteria

A.G. Soriano-Sánchez, C. Posadas-Castillo*, M.A. Platas-Garza, D.A. Diaz-Romero

Universidad Autónoma de Nuevo León - Facultad de Ingeniería Mecánica y Eléctrica (UANL-FIME), Mexico

Received 22 September 2014; received in revised form 16 January 2015; accepted 31 January 2015
Available online 9 February 2015

Highlights

- Synchrony is verified by the convergence of the synchronization error system.
- The coupling strength was obtained from the synchronization error system.
- Selection criteria based on energy and spectral characteristics are proposed.
- The selection of the chaotic signal was improved by the criteria proposed.
- The encryption, transmission and retrieval using chaotic signals were performed.

Abstract

Using a multi-scroll oscillator with an adjustable number of scrolls as chaos generator, this paper shows how an adequate control of the chaotic masking signal provides the basis for an improved security in private communication. We base the selection of the masking signal on two criteria related, respectively, to the energy and the spectral location of the signals in the complex synchronization network. The result is a successful encryption, transmission and retrieval of a confidential message in a two-channel communication system with multi-user modality.

Keywords: Private communications; Chaotic encryption; Multi-scroll chaotic oscillators; Synchronization; Complex network

1. Introduction

Mankind has developed increasingly complex ways to encrypt sensitive data. Chaos as a means of encryption represents a promising approach among the methodologies explored to veil information. Chaotic oscillators have received particular attention in the last decade or two because of their potential application to private communications. These systems have attracted the interest of researchers who have studied and implemented them in the field of communications [30].

Researchers appreciate the non-periodicity and apparent randomness of chaotic signals [9]. Nevertheless, this encryption process lacks a selection criterion to choose a suitable cloaking chaotic signal satisfying the message

* Correspondence to: Av. Pedro de Alba s/n, Cd. Universitaria, San Nicolás de los Garza N.L., C.P. 66451, Mexico. Tel.: +52 81 83294020x5755.
E-mail addresses: allansori@gmail.com (A.G. Soriano-Sánchez), cornelio.posadascs@uanl.edu.mx (C. Posadas-Castillo), miguel.platasg@uanl.mx (M.A. Platas-Garza), david.diazrr@uanl.edu.mx (D.A. Diaz-Romero).

http://dx.doi.org/10.1016/j.matcom.2015.01.007

requirements, i.e. the correct masking in time and frequency domain. Nowadays, the selection process of the chaotic signal is carried out through trial and error.

In 1990, for the first time, L.M. Pecora and T.L. Carroll synchronized two identical chaotic oscillators with different initial conditions [17]. The bases of chaos synchronization and its applications were established some years later. In 1994, C.W. Wu and L.O. Chua defined important concepts such as asymptotic synchronization, partial synchronization and synchronization error bounds. They also established the relation between asymptotic synchronization and asymptotic stability [28]. In 1995, J.F. Heagy et al. investigated the role of unstable periodic orbits in synchronous chaotic behavior [6]. They proved how desynchronized bursting behavior is initiated. They also suggested taking this phenomenon into account to yield high quality chaotic synchronization.

In 1996 N.F. Rulkov discussed the cooperative behavior related to the regimes of synchronized chaos [20]. Rulkov outlined some examples that illustrate different types of identical chaotic oscillations. In 1997 L.M. Pecora et al. reviewed the basics of chaotic synchronization such as stability criteria and generalized synchronization. They examined coupling configurations as well as secure communication schemes [18]. The same year, G. Kulumbán et al. provided a unified approach for the analysis and comparison of conventional and chaotic communications systems. In this work, they clarified the role of synchronization for chaotic communications and described chaotic synchronization schemes [8]. In 2001, S. Yanchuk et al. analyzed the mechanisms of desynchronization for a system of two coupled identical oscillators. They also reported on the transverse stability properties for the equilibrium point in coupled system [33].

Recently, new encryption techniques and communication schemes have been formulated. Some schemes generate pseudo-random sequences by iterating chaotic maps to encrypt image blocks [10]. The aim was to generate pseudo-random sequences with high initial-value sensitivity and good randomness. Some focused on the robustness and security [2]. In order to increase the security of the algorithm, the size of the key space and the complexity of the coupling parameters were increased. Readers interested in this topic are referred to [11,21,22] and references therein.

On the other hand, several methods have been proposed to achieve chaotic synchronization. In [4], N. Chopra demonstrated output synchronization for input–output passive systems and included the practical case of constant time delays in communication. M. Zribi et al. suggested sliding modes to synchronize a pair of unified chaotic oscillators [35]. For different parameters, the chaotic oscillator exhibited the behaviors of the Lorenz, Lü and Chen attractors, respectively. The effectiveness of the sliding mode controller was shown through the synchronization error. L. Torres et al. proposed the synchronization of a chaotic oscillator using an exponential nonlinear observer [24]. They concentrated on generalized synchronization with a master–slave configuration and parametric identification.

Some other techniques that can be found are: chaotic synchronization through adaptive control [32], synchronization via dynamic feedback controller [16], chaotic synchronization via the coupling matrix [23], chaotic synchronization via full (reduced) observer [15], modified projective phase synchronization [13], chaotic synchronization via nonlinear adaptive-impulsive control [25], chaotic synchronization through high-order control [3] and synchronization through discontinuous dynamical systems theory [12] for instance.

In this work, selection criteria for chaotic signals based on their energy and spectral characteristics are proposed. To achieve the purpose of this research, synchronization of chaotic oscillators is needed, for this reason, some results of synchronization of complex networks, which are constituted by chaotic oscillators, are presented. As final result, encryption, transmission and retrieval of a confidential message, using chaotic signals, is presented. The communication process is performed in a two-channel system with multi-user modality.

The present work uses the generalized Chua's oscillator [31]. This oscillator is of special interest because of the complex structure of its chaotic attractors. The Chua's oscillator produces a so-called multi-scroll attractor. Its generalized form allows us to vary the number of scrolls by modifying particular parameters. In this way, the variety, the complexity and intensity of the chaotic masking signal can be adjusted as additional breaking points are introduced.

To achieve synchronization, the coupling strength is computed from the stability analysis of the synchronization error system of the variables involved. This is an alternative way proposed by the present authors. It gives a value that has proven to be sufficient to achieve synchronization. The alternative computed value has two important characteristics: first, it is smaller than the commonly used value. For example the value calculated in Wang & Chen [27]; second, it is big enough to hold synchronization that results in the convergence to equilibrium of the synchronization error system. Simulations of the time evolution of the synchronization error variables are provided to verify the effectiveness of proposed value, which is another contribution of this paper.