Commun Nonlinear Sci Numer Simulat 19 (2014) 1424–1432

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

On observer-based secure communication design using discrete-time hyperchaotic systems

Rania Linda Filali [a,b,*], Mohamed Benrejeb [a], Pierre Borne [b]

[a] LA.R.A, Automatique, Ecole Nationale d'Ingénieurs de Tunis, BP 37, Le Belvédère, 1002 Tunis, Tunisia
[b] LAGIS, Ecole Centrale de Lille, BP 48, 59651 Villeneuve d'Ascq Cedex, France

ARTICLE INFO

Article history:
Received 2 May 2012
Received in revised form 9 November 2012
Accepted 2 September 2013
Available online 15 October 2013

Keywords:
Cryptosystems
Linear-state-observer
Synchronization of discrete-time hyperchaotic systems
Aggregation techniques
Benrejeb arrow form matrix

ABSTRACT

Stabilization conditions are proposed in this paper for master and slave hyperchaotic discrete-time systems synchronization. They are based on the use of an hyperchaotic observer system for variables estimation and of the aggregation techniques for stability study associated to the Benrejeb arrow form matrix for system description. Numerical simulation results illustrate the efficiency of these conditions and the success of message signal transmission for the considered cryptosystem communication, based on third order generalized hyperchaotic Hénon maps as transmitter and receiver key.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

Chaotic signals are irregular, aperiodic, low autocorrelated, broadband, and unpredictable, and these properties satisfy requirements for secure communication systems. Moreover, since chaotic systems are extremely sensitive to initial conditions and parameter variations, its application to cryptography, provides a great deal of interests, especially after the pioneering work done by Carroll and Pecora on successfully synchronizing two identical chaotic systems with different initial conditions [1,2]. Recently, many secure communication schemes based on chaotic synchronization have been proposed: chaotic masking, [3], parametric modulation method [4,5], chaotic modulation [6,7], inclusion approach [8] and chaotic shift keying [9]. Inspired by cryptosystems used in previous works [10,11], an application to discrete-time hyperchaos-based cryptography which is a combination of a classical cryptographic technique and synchronization is considered. For chaos synchronization, many approaches have been also regarded as special cases of linear or nonlinear observer design problems [10–17].

In this paper, the key idea for synchronization is to consider the slave system as linear-state observer of the state of the master. It guarantees synchronization of a class of high dimensional discrete-time hyperchaotic systems via a scalar transmitted signal.

Based on aggregation techniques for stability study and the Benrejeb arrow form matrix for system description [18–22], sufficient conditions are proposed for the linear-state observer design. They are inspired from previous results on synchronization studies of continuous chaotic processes [23–26].

* Corresponding author at: LA.R.A, Automatique, Ecole Nationale d'Ingénieurs de Tunis, BP 37, LeBelvédère, 1002 Tunis, Tunisia. Tel.: +216 71 874 700.
E-mail addresses: rania.filali@ec-lille.fr (R.L. Filali), mohamed.benrejeb@enit.rnu.tn (M. Benrejeb), pierre.borne@ec-lille.fr (P. Borne).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.09.005

The paper is organized as follows. In Section 2, a secure communication scheme combining conventional cryptographic methods and synchronization of discrete-time hyperchaotic systems is considered without considering transmission noise. In Section 3, for discrete-time hyperchaotic systems, the well-known concept of linear observer is introduced to formalize the problem of hyperchaos synchronization. By following this approach, sufficient conditions have been developed for asymptotic stabilization of the synchronization error system between two identical hyperchaotic discrete-time processes. These processes can't only reach chaos synchronization between two identical chaotic systems, starting with different initial conditions, but, also, can be applied to the proposed chaos based secure communication. In order to show the effectiveness of the developed technique, the case of the use of the third order discrete-time hyperchaotic Hénon systems is studied, in Section 4. In Section 5, numerical simulations are carried out using this kind of discrete-time hyperchaotic systems and the proposed secure communication scheme; then, some concluding remarks are given.

2. Hyperchaotic secure communication via linear-state-observer-based-synchronization. Problem statement

In this section, a discrete-time hyperchaotic secure communication, called hyperchaotic cryptosystem, shown in Fig. 1, is presented using a combination of a classical cryptographic technique and observer-based synchronization [10]. The master–slave hyperchaotic synchronization is based on a linear-state-observer design method, as shown in Fig. 1, allowing the hyperchaotic receiver to recover the information signal without noise such that $y_m(k) = y_s(k)$. The proposed scheme incorporates encrypter and decrypter blocs which respectively contain hyperchaotic master and slave systems.

- The hyperchaotic master system is described, in state space, by:

$$\begin{aligned} x_m(k+1) &= Ax_m(k) + f(x_m(k)) + \alpha NV(k) \\ y_m(k) &= Cx_m(k) + \alpha V(k) \end{aligned} \tag{1}$$

where $x_m(kT)$ is the state vector, noted $x_m(k)$ at instant kT, T the sampling time, $x_m \in R^q$. $A = \{a_{ij}\}$ a $(q \times q)$ constant matrix, $C = [c_1 \ldots c_q]$, a $(1 \times q)$ satisfying master–slave synchronization to be determined, $N = [n_1 \ldots n_q]^T$, a constant vector characterizing the way to mix the ciphertext $V(k)$ with the chaotic signal $x_m(k)$, α a scaling factor chosen to allow the term $\alpha NV(k)$ to belong to a compatible range with respect to the minimum and maximum bound of states variables of master and save chaotic signal $V(k)$ [27] and $f(x_m(k))$ a nonlinear vector function.
The considered hyperchaotic master system 1 generates the output signal $y_m(k)$ and the key $K(k)$ used $n$times as a keystream to encrypt the original message $m(k)$ with an encryption rule $en(\cdot)$, an n-shift cipher algorithm [28], such as:

$$V(k) = en(m(k), K(k)) = \underbrace{f_1(\ldots f_1(f_1}_{n}(m(k), \underbrace{K(k)), K(k)), \ldots, K(k))}_{n} \tag{2}$$

with:

$$K(k) = \sqrt{|x_{m1}(k) + x_{m2}(k) + \ldots + x_{mq}(k)|} \tag{3}$$

$x_{mi}(k), \forall i = [1 \ldots q]$ are elements of vector x_m.
$f_1(\cdot)$ is a non-linear function defined, in this case, by:

$$f_1(m(k), K(k)) = \begin{cases} m(k) + K(k) + 2h, \text{ for } -2h \leqslant m(k) + K(k) \leqslant -h \\ m(k) + K(k), \text{ for } -h < m(k) + K(k) < h \\ m(k) + K(k) - 2h, \text{ for } h \leqslant m(k) + K(k) \leqslant 2h \end{cases} \tag{4}$$

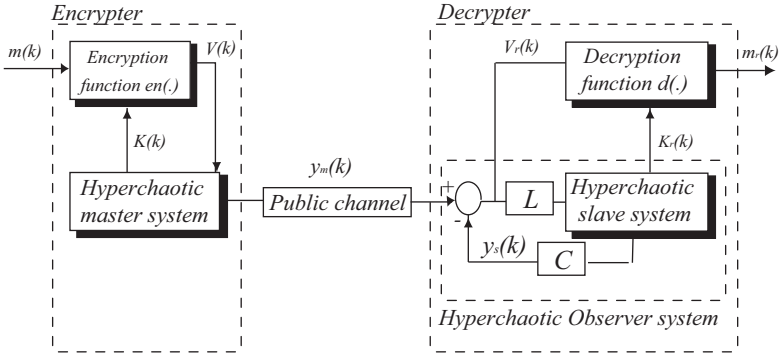

Fig. 1. Block diagram of the proposed hyperchaotic communication based on cryptography.

Download English Version:

https://daneshyari.com/en/article/755828

Download Persian Version:

https://daneshyari.com/article/755828

Daneshyari.com