Applied Mathematics and Computation 246 (2014) 711–730

Contents lists available at ScienceDirect

Applied Mathematics and Computation

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

A new approach for secure communication using constrained hyperchaotic systems

Mohamed F. Hassan

Electrical Engineering Department, College of Engineering, Kuwait University, P.O. Box: 5969, Safat 13060, Kuwait

ARTICLE INFO

Keywords:
Chaos
Chaotic synchronization
Constrained state estimation
Nonlinear systems
Secure communication

ABSTRACT

In this paper, a new technique is developed for a typical secure communication scheme. In this approach, we introduce the concept of constrained hyperchaotic systems to encrypt the carrier of the data signal to be transmitted. At the transmitter end, two different chaotic oscillators are coupled, constrained and used as a new hyperchaotic system. One of the outputs of the constrained hyperchaotic system is used as a carrier for the encrypted data. Then, the outputs of the system, including the modulated carrier, are encrypted using a set of pre-defined encryption rules. At the receiving end, and after decrypting the received outputs, the discrete-time *Constrained Regularized Least Square* (CRLS) estimator is used to reconstruct the constrained hyperchaotic signals, and hence retrieve the transmitted data. Simulation results are presented to illustrate the capability of the CRLS estimator in reconstructing the states of the constrained hyperchaotic system. Moreover, the proposed secure communication scheme is applied to transmit discrete images for which the quality of the transmission process is measured by the bit-error rate (BER).

1. Introduction

Since the proliferation of wireless production, secure communication has become one of the very important research topics and has received great attention. The introduction of chaos into communication systems offers several opportunities for improvement. The practical unpredictability of chaotic dynamics, its complexity, and the possibility of synchronizing chaotic systems are the elements giving the potential for the application of chaos in secure communication schemes. Moreover, the random behavior of chaotic systems can be very useful in distinguishing modulation as noise [1,2].

Compared to conventional communication systems, chaotic based communication systems acquire potential benefits [2,3]. From these are secure communications, utilization of the intrinsic nonlinearities in communication devices, efficient use of the bandwidth of the communication channel, large signal modulation for the efficient use of carrier power, and the dependency of chaotic signal on initial conditions make it difficult to predict. Moreover, chaotic systems share many properties of stochastic processes which are basic requirements of the spread spectrum communication.

Chaotic communication systems are designed and implemented either with chaos synchronization or without chaos synchronization [4–9]. However, most of the work done in this area is based on chaos synchronization between two chaotic systems generally called driver (master) and response (slave). Different techniques have been proposed for chaos synchronization. Among these techniques are nonlinear control [10–12], adaptive synchronization [13,14], backstepping control [15], passive control [16], sliding mode control [17–19], control Lyapunov function (CLF) [20,21], fuzzy control

E-mail addresses: m.fahim@ku.edu.kw, m.f.hassan47@gmail.com

http://dx.doi.org/10.1016/j.amc.2014.08.029
0096-3003/

[22], digital redesign approach [23], impulsive control [12,24,25], extended Kalman filter [1,26], observer-based synchronization [27–29], projective synchronization [30–32], finite-time control [33], active control [34], delayed feedback control [35,36], quadratic optimal control [37], and so on.

Masking the contents of a message using chaotic signals have been achieved using different methods [4–8,10,38,39]. However, it has been shown that most of these techniques are not secure since it is possible to extract the encoded message from the transmitted chaotic signal by using different unmasking techniques [10]. To avoid this problem, different approaches have been developed to design cryptosystems based on chaos [1,4,5,10]. In these approaches, conventional cryptographic methods and synchronization of chaotic systems are combined in order to enhance the security level of transmitted chaotic signals.

In this research work, we introduce a new approach for secure data communication in which another level of security is added to the data transmission system. More specifically, we encrypt the type of the chaotic oscillator generating the carrier for the data to be transmitted. Such an approach is done by imposing a set of equality and/or inequality constraints to the generated chaotic signal. The resulting chaotic signals have waveforms and wave patterns that are different from those generated from the original chaotic oscillator. Moreover, by changing the set of constraints from one time period to another, we achieve another form of the generated chaotic signals. Therefore, the type of the chaotic oscillator is hidden and more importantly, synchronization of the chaotic signal can never be achieved without the knowledge of the set of imposed constraints.

In this paper, the hyperchaotic Chen system and the unified chaotic system with adaptive parameter are coupled to create a new hyperchaotic system [18]. The generated chaotic signals resulting from the new hyperchaotic system are encrypted by imposing a set of linear and/or nonlinear, equality and/or inequality constraints to the system model. This leads to chaotic signals with waveforms and wave patterns different from those generated either from each individual chaotic system or from the unconstrained coupled hyperchaotic system. To increase the security level, the set of constraints and their upper and/or lower bounds (which can be either constants or time dependent functions), can be changed from one time interval to another during the data transmission period. Since the generated chaotic signals will not follow any typical chaotic system, they cannot be synchronized without the knowledge of the chaotic oscillator and the imposed set of constraints. Realizing that neither online control approaches nor estimation techniques available in the literature can deal with constrained nonlinear dynamical systems, the CRLS estimator is used to handle this problem. Therefore, at the receiving end, the CRLS estimator is used as a driver to reconstruct the carrier generated at the transmitting end and hence extract the encoded data. It is worth mentioning that the set(s) of constraints, their bounds, and the set of encryption rules have to be agreed upon between the transmitter and the receiver.

The rest of the paper is organized as follows. Section 2 briefly describes the unified chaotic system and the hyperchaotic Chen system. The outline of the proposed secure communication scheme is formulated in Section 3. The discrete-time constrained nonlinear estimation problem is presented in Section 4. The CRLS estimator is presented and analyzed in Section 5. Section 6 is devoted to the presentation of the numerical results that show the effectiveness of the CRLS estimator and hence the proposed secure communication scheme in transmitting three discrete images. Finally, some concluding remarks are given in Section 6.3.

2. System description

2.1. The unified chaotic system

The model of the unified chaotic system is given by [12,16,18,20]:

$$\begin{aligned}\dot{x}_{u1} &= (25\alpha + 10)(x_{u2} - x_{u1})\\ \dot{x}_{u2} &= (28 - 35\alpha)x_{u1} - x_{u1}x_{u3} + (29\alpha - 1)x_{u2}\\ \dot{x}_{u3} &= x_{u1}x_{u2} - ((8+\alpha)/3)x_{u3}\end{aligned} \tag{1}$$

The discretized form of (1), using first order approximation (Euler method), is such that:

$$\begin{aligned}x_{u1k+1} &= x_{u1k} + \Delta T(25\alpha + 10)(x_{u2k} - x_{u1k})\\ x_{u2k+1} &= x_{u2k} + \Delta T(28 - 35\alpha)x_{u1k} - \Delta T x_{u1k}x_{u3k} + \Delta T(29\alpha - 1)x_{u2k}\\ x_{u3k+1} &= x_{u3k} + \Delta T x_{u1k}x_{u2k} - ((8+\alpha)/3)\Delta T x_{u3k}\end{aligned} \tag{2}$$

where $\boldsymbol{x}_{\boldsymbol{uk}} \in \boldsymbol{R}^3$ is the state vector, $\alpha \in [0,1]$ is the system parameter, and ΔT is the sampling time period. The system described by (2) is chaotic for any value of $\alpha \in [0,1]$. The system (2) is the generalized Lorenz chaotic system for $0 \leqslant \alpha < 0.8$. It is Lu chaotic system when $\alpha = 0.8$, and it is the generalized Chen chaotic system when $0.8 < \alpha \leqslant 1$.

The output of the system $\boldsymbol{y}_{\boldsymbol{uk}+1} \in \boldsymbol{R}^2$ is given by:

$$\boldsymbol{y}_{\boldsymbol{uk}+1} = [0.1\ 0.1\ 0]\boldsymbol{x}_{\boldsymbol{uk}+1} \tag{3}$$