Information Sciences 305 (2015) 146–164

Contents lists available at ScienceDirect

Information Sciences

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

# A general hybrid model for chaos robust synchronization and degradation reduction

Yashuang Deng [a,b], Hanping Hu [a,b,*], Naixue Xiong [c], Wei Xiong [a,d], Lingfeng Liu [e]

[a] School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China
[b] Key Laboratory of Image Processing and Intelligent Control of Education Ministry, Wuhan 430074, China
[c] School of Computer Science, Colorado Technical University, Colorado Spring, CO, USA
[d] Computer Teaching and Experiment Center, South-Central University for Nationalities, Wuhan 430074, China
[e] School of Software, Nanchang University, 330099, China

ARTICLE INFO

*Article history:*
Received 12 June 2014
Received in revised form 21 January 2015
Accepted 30 January 2015
Available online 7 February 2015

*Keywords:*
Chaotic system
Robust synchronization
Finite precision
Dynamical degradation
Hybrid model

ABSTRACT

This paper focuses on the problem of robust synchronization of uncertain continuous chaos and dynamical degradation of digital chaos. A hybrid model is established based on the complementarities between continuous chaos and digital chaos. An impulse-like controller along with a state feedback controller is designed to guarantee the robust synchronization of uncertain continuous chaotic systems and reduce the dynamical degradation of digital chaotic systems respectively. Simulation studies are conducted to illustrate the effectiveness of the hybrid model. Compared with the existing synchronization schemes, this model can realize the synchronization of two uncertain continuous chaotic systems without transmission of synchronization control signals and has better robustness. Meanwhile, it can make the properties of given digital chaotic systems achieve desirable levels, while the existing remedies for digital chaotic systems fail to. Thus, the hybrid model is very applicable to cryptography, secure communication and other potential applications.

© 2015 Elsevier Inc. All rights reserved.

## 1. Introduction

Over the past two decades, chaos has sparked much interest in the area of information security and related fields especially in cryptography and secure communication. Actually, there exists a tight relationship between chaos and cryptography [2,13]. Some properties of chaotic systems are just consistent with two classical cryptography principles "confusion" and "diffusion" proposed by Shannon [31]. In general, there are two main design patterns for chaotic cryptography: pure digital chaotic cipher and chaos synchronization-based secure communication.

In the first pattern, digital chaotic systems which are usually realized by computers or digital devices, are easily reproducible and stable. Since the first chaotic stream cipher was proposed by Mathews in 1989 [25], large numbers of digital chaotic cryptographic algorithms have emerged and been analyzed [7,8,12,36,37]. Unfortunately, researchers have found that many chaotic cryptographic algorithms are not secure due to the dynamical degradation of digital chaos induced by finite precision realization [4,17,38]. The degradation behaviors often refer to properties of short cycle, low complexity, bad distribution and correlation [3,15,29]. Researchers have provided some countermeasures, such as using higher computing precision [39], cascading multiple chaotic systems [9] and perturbing the chaotic system [14,16,23]. The perturbation-based scheme

* Corresponding author at: School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China.
*E-mail addresses:* dys0377@163.com (Y. Deng), hphu@mail.hust.edu.cn (H. Hu).

http://dx.doi.org/10.1016/j.ins.2015.01.028
0020-0255/© 2015 Elsevier Inc. All rights reserved.

can greatly improve the dynamical degradation of digital chaotic systems and has been proved to perform better than the first two methods [15]. However, the properties of perturbed system are dominated by the perturbing source (like linear shift register). Another widely used method is switching multiple chaotic systems [26,41], which can greatly increase the cycle length and weaken the correlation of output sequence. However, this method depends deeply on the applied switching law. The error compensation method proposed by Hu et al. [10] is also an effective way to deal with the degradation of digital chaotic systems since it can drive most properties of the compensated digital chaotic map to be approximate to the original chaotic ones. However, it seems difficult to extend this method to higher dimensional cases. Generally, the above solutions mainly focus on the compensation of properties of digital chaotic systems and can only make the properties of digital systems approximate to the original chaotic ones. In this way, modified digital chaotic systems are still vulnerable to attacks owing to the biases (like obvious structural characteristic) existing in the original chaotic systems. Furthermore, these methods cannot drive the properties (like complexity) of systems to achieve some expected levels, which may not be desirable for some applications. Therefore, one should resort to other solutions to ensure the expected properties, such as uniform distribution, higher complexity and ergodicity.

In the second pattern, continuous chaotic systems which are generally realized via analog circuits, can preserve rich chaotic dynamical properties. They have been widely used in chaos synchronization-based secure communication [21] and other potential applications such as those in the biological and medical systems, especially for human brain and heartbeat regulation. In 1990, the pioneer work of Pecora and Carroll [28], Ott et al. [27] has made a major breakthrough for chaotic secure communication. Since then, large numbers of control methods have been proposed and used for chaos synchronization, such as feedback control [11,34], tracking control [18,24], sliding-mode control [1,20], impulsive control [6,30], fuzzy control [5,32,35], projective control [19,22] and coupling control [33]. Especially, the robust synchronization of nonlinear systems with parameter uncertainties has gained a great deal of interest [1,18,20,24,42,43]. It is impractical to assume ideal conditions such as designed parameter values and identical systems, which often make the system synchronization invalid due to the effect induced by noise. Moreover, in existing chaos synchronization schemes, continuous or impulsive synchronization control signals must be transmitted to ensure chaos synchronization, which certainly increases the bandwidth occupancy and leads to information leakage. The key information (like system parameters) of chaotic system can be estimated via nonlinear prediction technology and other methods, thereby leading to a security risk [40]. Consequently, it is important and meaningful to resort a synchronization method to assure robust synchronization of uncertain chaotic systems for a long time with less or even no transmission of synchronization control signal.

Note that there exist complementarities between digital and continuous chaotic systems: digital chaotic systems can easily keep synchronization for a long time given the same system and initial value but often suffer from dynamical degradation due to finite computing precisions. Continuous chaotic systems can preserve rich dynamical properties but it is difficult to keep long time stable synchronization owing to parameter uncertainties. Based on these complementarities, we establish a hybrid model by coupling digital chaotic system and continuous chaotic system. This model contains a pair of continuous chaotic systems and a pair of digital chaotic systems. Each side of digital chaotic system is utilized to control the local continuous chaotic system to ensure synchronization. Meanwhile, each continuous chaotic system is sampled in turn to anti-control the corresponding digital chaotic system to prevent the dynamical degradation. The hybrid model can deal with the problem of robust synchronization of continuous chaos and the dynamical degradation of digital chaos in the same framework. Better than the existing synchronization approaches, our synchronization scheme can realize synchronization of two uncertain chaotic systems without transmission of any synchronization control signal, which certainly enhances the security of system indirectly and makes the model own better robustness. Besides, the model cannot only make the digital system behave chaotically again but also ensure that the digital system owns desirable properties rather than the original ones, thereby avoiding the biases of original chaotic systems and enhancing the security of the digital chaos-based processing. In this way, it performs better than the existing remedies for digital chaotic systems. Thus, the proposed hybrid model is very proper for cryptography, pseudorandom coding, secure communication and other potential applications.

The rest of this paper is organized as follows: the problem statement and preliminaries are given in Section 2. Section 3 introduces the basic mechanism of the hybrid model, and in Section 4 the illustration example is presented to show the efficiency of the hybrid model, and performance comparisons with existing results are made. Finally, we conclude this paper in Section 5.

## 2. Problem statement and preliminaries

In this section, we give a brief description of the dynamical degradation of digital chaotic systems and the synchronization robustness of uncertain continuous chaotic systems.

Consider a digital chaotic system:

$$X_{i+1} = F_L(X_i) \tag{1}$$

where $X_i \in \Omega_L$ is a digital state vector and $\Omega_L$ is the finite version of real set $\Omega \subset R^m$ . $L$ is the computing precision. $F_L = B_L \circ F : \Omega \to \Omega_L$ is the digital chaotic map, $F : \Omega \to \Omega$ is a chaotic map, $B_L : \Omega \to \Omega_L$ is a quantization function and there are three widely used forms for almost all computer algorithms [17]: $floor_L(\cdot)$, $round_L(\cdot)$ and $ceil_L(\cdot)$.

Download English Version:

https://daneshyari.com/en/article/393067

Download Persian Version:

https://daneshyari.com/article/393067

Daneshyari.com