Chapter 14

Secure Digital Data Communication Based on Fractional-Order Chaotic Maps

Hamid Hamiche
Mouloud Mammeri University, Algeria

Sarah Kassim
Mouloud Mammeri University, Algeria

Ouerdia Megherbi
Mouloud Mammeri University, Algeria

Said Djennoune
Mouloud Mammeri University, Algeria

Maamar Bettayeb
Sharjah University, UAE

ABSTRACT

The aim of the chapter is twofold. First, a literature review on synchronization methods of fractional-order discrete-time systems is exposed. Second, a secure digital data communication based on synchronization of fractional-order discrete-time chaotic systems is proposed. Two synchronization methods based on observers are proposed to synchronize two fractional-order discrete-time chaotic systems. The first method concerns the impulsive synchronization where sufficient conditions for the synchronization error of the states are given. The second method concerns the exact synchronization which is based on a step-by-step delayed observer. In the same way, conditions are provided in order to allow the reconstruction of the states and the unknown input which is the message in this case. The two synchronization methods are combined in order to design a novel robust secure digital data communication. The performance of the proposed communication system is illustrated in numerical simulations where digital image signal is considered.

DOI: 10.4018/978-1-5225-5418-9.ch014
1. INTRODUCTION

Fractional-order differentiation and integration operators become useful mathematical tools in many areas of science and engineering (Kilbas et al., 2006). In recent years, attention has been brought on the investigation of the chaotic behavior of fractional-order systems.

For continuous-time systems, the basic idea is to replace the integer-order derivative by a fractional-order derivative in some well-known nonlinear chaotic integer-order systems. Among the continuous-time fractional-order chaotic systems proposed in the literature, one can find the Chua’s system, the Newton-Leipnik’s system, the Lorenz system (Sabatier et al., 2007). Meanwhile, with the rapid growth of the fractional-order calculus, some researchers are devoted to practical applications, such as the fractional-order PID controllers (Podlubny, 1999), the fractional-order signal processing, (Sejdic et al., 2011), fractional calculus to fluid mechanics, (Kulish & Jose, 2002), fractional calculus to polymer science, (Douglas, 2007) etc. Recently, some works are devoted to the application of the fractional-order (discrete-time or continuous) chaotic systems in secure communication (Gao et al., 2011; Kiani et al., 2009; Odibat, 2010; Zhang and Yang, 2011; Zhou and Ding, 2012). Indeed, with the rapid progress of communication network and information technology, several standard encryption methods have been developed. In the early 1970, the Data Encryption Standard (DES) algorithm has been proposed (DES, 1977). Due to the short length of its key, this algorithm has been replaced by the Advanced Encryption Standard (AES) (Daemen and Rijmen, 2002). These algorithms belong to the symmetric encryption category. They are called so, because they require the same secret key for both encryption and decryption. On the other hand, another algorithms category uses different keys for encryption and decryption. It is qualified as asymmetric encryption category. The RSA algorithm is the most known algorithm in this category (Rivest et al., 1978). Unfortunately, for complex data secure transmission especially images security, the cited methods may not be the most desired candidates because they suffer from many issues, such as bulk volume of data, high correlation among adjacent pixels, high redundancy and real time requirement. To overcome these limitations, chaos based cryptography has been considered. Since then, this field becomes a new interesting research topic and several new schemes have been established. The most recent chaotic cryptosystems use fractional-order chaotic systems instead of the integer order ones. The major advantage of using fractional-order chaotic systems in secure data transmission is the improved security. We can explain this by the fact that fractional order chaotic system based transmission scheme has supplementary secret keys which are its fractional orders (Hamiche et al., 2015b; Kassim et al., 2016; Kassim et al., 2017). Then, with the consideration of chaotic features and the performance of algorithms, lots of novel encryption algorithms based on fractional-order chaotic systems have been proposed (Gao et al., 2011; Xu et al., 2014; Zhen et al., 2013; Zhen et al., 2012). As for the integer-order case, the fractional-order chaotic systems used at the transmitter and receiver levels should be synchronized in order to retrieve the sent original message. This is why, many synchronization approaches already proposed to synchronize integer-order chaotic systems have been generalized for the fractional-order ones. For instance, we can mention the sliding mode synchronization (Muthukumar et al., 2015), the impulsive synchronization method (Andrew et al., 2015), the active synchronization method (Agraval et al., 2012) and the adaptive synchronization method (Zhou and Bai, 2015). It should be noted that the search in secure digital data based on the synchronization of fractional order chaotic systems is focused on the continuous case. On the other hand, the search in the discrete case is very limited. Indeed, except...
Related Content

Design Churn as Predictor of Vulnerabilities?
www.igi-global.com/article/design-churn-as-predictor-of-vulnerabilities/118146?camid=4v1a

Resource Analysis and Classification for Purpose Driven Value Model Design
www.igi-global.com/article/resource-analysis-classification-purpose-driven/40953?camid=4v1a

An Agent Based Formal Approach for Modeling and Verifying Integrated Intelligent Information Systems
www.igi-global.com/chapter/agent-based-formal-approach-modeling/23793?camid=4v1a