Chapter 97
Novel Cryptography Technique via Chaos Synchronization of Fractional-Order Derivative Systems

Alain Giresse Tene
University of Dschang, Cameroon

Timoleon Crépin Kofane
University of Yaounde I, Cameroon

ABSTRACT

Synchronization of fractional-order-derivative systems for cryptography purpose is still exploratory and despite an increase in cryptography research, several challenges remain in designing a powerful cryptosystem. This chapter addresses the problem of synchronization of fractional-order-derivative chaotic systems using random numbers generator for a novel technique to key distribution in cryptography. However, there is evidence that researchers have approached the problem using integer order derivative chaotic systems. Consequently, the aim of the chapter lies in coding and decoding a text via chaos synchronization of fractional-order derivative, the performance analysis and the key establishment scheme following an application on a text encryption using the chaotic Mathieu-Van Der Pol fractional system. In order to improve the level of the key security, the Fibonacci Q-matrix is used in the key generation process and the initial condition; the order of the derivative of the responder system secretly shared between the responder and the receiver are also involved. It followed from this study that compared to the existing cryptography techniques, this proposed method is found to be very efficient due to the fact that, it improves the key security.

DOI: 10.4018/978-1-7998-7705-9.ch097

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Nowadays, developing new strategies to protect sensitive information from eavesdropping has attracted significant attention in the worldwide communication networks. That is, wide investigations have been made to implement an effective cryptosystem to ensure information encryption and decryption. These include the algorithmic key based encryption systems which usually consider a digital stream and convolute it with a given binary pattern using as the key. This encryption method can be denoted as the Vernam Cipher method (Bloisi and Iocchi 2007). In this method, the message is transformed to a binary string (a sequence of 0 and 1), and the key is a randomly generated sequence of 0 and 1 having the same length as the message. The encryption is done by adding the key to the message modulo 2 bit by bit, this includes the symmetric key encryption such as the Data Encryption Standard (DES) cryptosystem (Standard 1977), the Advanced Encryption Standard (AES) (Standard 2001) cryptosystems, etc. Even though this encryption method has been used for long times and is still used today, it presents some lacks in the key security and the key distribution. The drawback of this encryption technique comes from the fact that, it is easily breakable even if the key can be used only one time (one time-pad key). However, this drawback has been avoided by developing other software cryptosystems that use asymmetric algorithms key distribution which is called a public key cryptography such as the Rivest Shamir Adleman (RSA), the Elliptic Curve Cryptography (ECC) cryptosystems just to name a few (Bleichenbacher 1998, Habib 2009). Such cryptosystems usually use several computational resources and compare them with their counterparts but they are not generally used to encrypt bulk data stream and are computationally hard. Although this encryption technique is not yet broken, further investigations have been made to develop another encryption method that is based on chaos. Chaos theory has simulated increasing attentions of scientists since the work of Lorenz (1963). Due to their random-like behavior, their unpredictability character and their high degree of nonlinearity, chaotic signals have been proven to be very efficient for information security then, in the recent few decades, chaos based cryptosystems which consists of masking an information to be transmitted through a chaotic signal have received a great deal of interest. Here one denotes the chaos masking (CMA) which consists of masking the plaintext through a chaotic signal, the chaos shift keying (CSK), the chaos modulation (CMO), etc (Annovazzi-Lodi *et al.* 2005, Dedieu *et al.* 1993, Tang *et al.* 2002). However, particular attentions have been given to the encryption technique based on chaos synchronization between distant elements in large networks in order to improve the effectiveness of information security. This encryption technique has been developed by several authors (Alvarez 2006) and has even been implemented in the real experiment. These authors demonstrated that a cryptosystem based on this encryption is highly efficient, although it is difficult to synchronize two chaotic systems. Therefore, this method consists of generating an encryption key by synchronizing two chaotic signals (driver and responder systems). Thus, the aim of this chapter is to develop new strategy of key encryption based on chaos synchronization of two chaotic systems with fractional order derivative in order to improve the information security.

The main motivation behind such an idea includes the fact that, the fractional order derivative chaotic system is geometrically complex and its high nonlinearity degree makes such a system an efficient tool to encrypt message. Furthermore, the order of the derivative might be used as the secret key as well as other parameters of the system enhancing the effectiveness of the encryption method. In addition, it was shown by Tene & Kofane (2017) that the fractional order of the derivative can induce quick synchronization of chaotic systems which can highly improve the encryption and decryption speed. Such encryption

32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/novel-cryptography-technique-via-chaos-synchronization-of-fractional-order-derivative-systems/270692

Related Content

Michigan vs. Pittsburgh Style GA Optimisation of Fuzzy Rule Bases for Gene Expression Analysis
Gerald Schaeferand Tomoharu Nakashima (2013). *International Journal of Fuzzy System Applications (pp. 60-72).*
www.irma-international.org/article/michigan-vs-pittsburgh-style-ga-optimisation-of-fuzzy-rule-bases-for-gene-expression-analysis/101770

Metaverse for Healthcare: Possible Potential Applications (Virtual Reality Technologies), Opportunities, Challenges, and Future Directions
Hafiz Asif, Rabia Zahid, Uzma Bashir, Waseem Afzal, Misbah Firdous, Ahsan Zahidand Muhammad Hasnain (2024). *Metaverse Applications for Intelligent Healthcare (pp. 274-305).*
www.irma-international.org/chapter/metaverse-for-healthcare/334353

Extending Loosely Coupled Federated Information Systems Using Agent Technology
Manoj A. Thomas, Victoria Y. Yoonand Richard Redmond (2007). *International Journal of Intelligent Information Technologies (pp. 1-20).*
www.irma-international.org/article/extending-loosely-coupled-federated-information/2420

Developmental Language Learning from Human/Humanoid Robot Social Interactions: An Embodied and Situated Approach
Artur M. Arsénio (2013). *Theoretical and Computational Models of Word Learning: Trends in Psychology and Artificial Intelligence (pp. 197-223).*
www.irma-international.org/chapter/developmental-language-learning-human-humanoid/74895

A Differential Evolution Based Multiclass Vehicle Detector and Classifier for Urban Environments
Deepak Dawarand Simone A. Ludwig (2018). *Intelligent Systems: Concepts, Methodologies, Tools, and Applications (pp. 1544-1569).*
www.irma-international.org/chapter/a-differential-evolution-based-multiclass-vehicle-detector-and-classifier-for-urban-environments/205846