Dynamics of Continuous, Discrete and Impulsive Systems
Series **B:** *Applications & Algorithms* **10 (2003)** 799-812

Digital Information Encryption Using Chaos Synchronization

H. Zhang, G. Zhou, Z. P. Jiang and Yao Wang

Department of Electrical and Computer Engineering
Polytechnic University
Six Metrotech Center
Brooklyn, NY 11201, U.S.A.

E-mail: zjiang@control.poly.edu

Abstract. In this paper, we present a novel digital encryption algorithm using discrete-time chaotic synchronization. The boundedness property of chaotic systems is exploited to realize the encryption and decryption procedure. Different from previous approaches of encrypting messages by chaotic systems, the proposed method focuses on digital signals instead of analog ones. Moreover, after synchronization, the transmitted signal has the same bit-length as the information data which is to be transmitted. The chaotic signal in the encryptor depends on the information message and cannot be predicted by the decryptor independently. Our simulation results based on an application to image encryption with Hénon map validate the proposed method.

Keywords. Discrete-time, chaos synchronization, digital encryption, feedback, observer.
AMS (MOS) subject classification: 34K23, 37N35, 68P25, 93C10, 93C55, 93C83, 93C95, 94A60.

1 Introduction

In the last decade, tremendous progress has been made on the topic of chaos synchronization and its potential applications to secure communication and data encryption; see [2, 4, 6, 7, 8, 9, 13, 16, 17, 20, 23, 24] and references therein. The properties of being aperiodic, unpredictable, noise-like, sensitive to disturbance and initial condition make chaotic signals a suitable candidate for encrypting messages. Moreover, as deterministic dynamical systems, chaos are easy to be managed in the analysis, design, and implementation of secure communication systems. Among the typical communication schemes with chaotic dynamics developed so far are chaotic masking [2], chaotic modulation [20], chaotic shift keying [6], and more recently, the impulsive synchronization method [21]. Chaotic masking, modulation and impulsive synchronization are usually concerned with the transmission of analog messages. For security and privacy purposes, the analog to-be-transmitted signals must retain the chaotic behavior and be much larger than the private message. Chaotic shift keying is used to transmit digital messages, by which every bit of digital message is represented by an analog waveform.