Dynamics of Continuous, Discrete and Impulsive Systems
Series **B:** *Applications & Algorithms* **10 (2003)** 221-234

A NEW CHAOTIC SYSTEM FOR BETTER SECURE COMMUNICATION [1]

Weiguang Yao, Chris Essex and Pei Yu

Applied Mathematics Department
University of Western Ontario, London, Ontario, Canada N6A 5B7

Abstract. A 4-dimensional nonlinear dynamical system is proposed for secure communications using chaos synchronization. It is shown that the chaotic attractor of the system has complex local structure that is sensitive to the perturbation of the system's parameters. With the aid of the nonlinear forecasting technique, these properties have proven to be very useful in improving the security of communications via chaos encryption.
Keywords. Chaos encryption, strange attractor, chaos synchronization, nonlinear dynamical forecasting, generalized competitive mode.
AMS (MOS) subject classification: 34C28, 34C60, 94A60.

1 Introduction

Recently, chaos synchronization has received considerable attention because of its potential applications to secure communications [1-9]. It is well known that two identical chaotic systems can be synchronized by giving one system information about the state of the other. Pecora and Carrol noticed that by adding a small amplitude message to a chaotic signal, the signal is still close enough to the exact chaotic mask to allow the two dynamical systems to synchronize [1]. Later, Cuomo and Oppenheim used the idea of chaos synchronization to develop a real circuit system for private communications [2,3]. By using the method of chaos masking, a message is not only carried by a chaotic signal, but is also masked by the carrier. It has been shown using the time series of an intercepted signal that the message is masked well because the magnitude of the carrier is much larger than that of the message. Furthermore, the study of the power spectrum of an intercepted signal indicates that the trace of the message is hidden well due to the the broadband spectrum of the chaotic carrier and the much smaller magnitude of the message. Therefore, this new method is expected to be used in secure communications. In addition, the sensitivity of synchronization to parameter perturbations may further increase the security of communications. In general, only identical or extremely close chaotic systems may be synchronized, which implies that it is very difficult for an eavesdropper to find a well

[1] Supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), and the Ontario Graduate Scholarship in Science and Technology (OGSST).