Chapter 21
Chaos Synchronization with Genetic Engineering Algorithm for Secure Communications

Sumona Mukhopadhyay
Army Institute of Management, India

Mala Mitra
Camellia School of Engineering and Technology, India

Santo Banerjee
Politecnico di Torino, Italy & Techfab, Italy

ABSTRACT

In this chapter, the authors have attempted to explore an association between chaos synchronization with genetic engineering algorithm. The authors developed a cryptographic technique using keys generated by time delayed synchronized systems by modifying the selection mechanism of the basic genetic algorithm. This has resulted into a proposed genetic engineering algorithm for cryptography which successfully deciphers the message. The observed results support the stated aim of the proposed genetic engineering algorithm that it is a reliable, effective and computationally cheaper substitute to the cryptography also developed here with ($\mu /p$, $\lambda$)- selection scheme of Evolutionary strategy. A detail study is also presented with the analysis.

1. CHAOS SYNCHRONIZATION AND CRYPTOGRAPHY

The turning point in traditional schemes of cryptography was brought about by the revolutionary work of Pecora and Carroll (Pecora & Carroll, 1990). This opened a gateway to varied areas of applications of chaos synchronization namely secure communication, chaos generators design, chemical reactions, biological systems, information science (Hramov & Koronovskii, 2005a; Garcia – Ojalia, & Roy, 2001; Yang & Chu 1997; Bowong, 2004; Kittel et al, 1994) and many more significant applications.

DOI: 10.4018/978-1-61520-737-4.ch021
Pecora and Carroll experimented on two systems producing their phenomenal work. The first is known as a driver and the other a response system. They used a novel idea of generating a chaotic signal to drive a non-linear dynamic system such that the state of the second system is governed by the state of the driving system. This is possible if the two systems are coupled by a proper controlling function. However, it is to be noted that the behavior and system parameters of the response system is dependent on the behavior of the driving system alone, similar to a master-slave relationship. When subjected to suitable conditions, the response system will exhibit a chaotic pattern which is in sync with the driver system. This phenomenon is known as chaos synchronization. Till now many different types of synchronizations have been analyzed in ordinary and time delayed dynamical systems such as complete synchronization (Fujisaka & Yamada, 1983), generalized synchronization (GS) (Rulkov et al, 1995; Kocarev & Parlitz, 1996; Hramov & Koronovskii, 2005a), generalized projective synchronization of a unified chaotic system (Yan and Li 2005), anticipated synchronization (AS) (Masoller, 2001), lag synchronization (LS) (Rosenblum et al, 1997; Zhan et al, 2002), phase synchronization (PS) (Rosenblum et al, 1996; Koronovskii & Hramov, 2004), antiphase synchronization (APS), time scale synchronization (Hramov et al, 2005b), intermittent generalized synchronization in which the authors (Hramov et al, 2005c) detected that before the transition of unidirectionally coupled chaotic oscillators to generalized synchronization, in some time intervals a non-synchronous behavior occurs and functional synchronization (FS) (Banerjee & Chowdhury, 2009).

Recent research on coupled non-linear systems proved that the properties of chaotic dynamics such as ergodicity (Caponetto et al, 2003) and sensitivity on initial conditions can be tapped for potential applications in secure communications around which this chapter primarily focuses on. The information signal is masked by a chaotic signal which forms a carrier and transmits the information signal in a secure way. The masking is removed at the receiver end. Even if the communication is intercepted, the information signal cannot be deciphered unless total information of the chaos signal generating system is at the disposal of the interpreter. A proper choice for the chaotic system must be made accurately for secure communication. Simple chaotic systems such as those having one positive Lyapunov exponent should be avoided for cryptographic purposes (Perez & Cerdeira, 1995). L. Pecora (Pecora, 1996) suggested that a chaotic system with at least two positive Lyapunov exponents should be an ideal choice. Such a chaotic system is known as a hyperchaotic system (Rossler, 1979), characterized by higher randomness and unpredictability which are vital for secure transmission of signals. Chaos theory has found its roots in secure communication due to its fundamental characteristics of sensitivity to initial conditions, ergodicity and mixing and several works have been discussed on combining features of chaos using both circuits and software simulations (Alvarez et al, 1999a; Alvarez et al, 1999b; Dachselt & Schwarz, 2001; Kocarev et al, 1998; Kocarev, 2001). The most attractive feature of chaotic system that makes it apt for novel engineering applications is its unpredictable and random nature. These are the key properties which are explored in communication theory for secure transmission of data as pointed out by Shannon (Shannon, 1949). To quote Shannon, “In a good mixing transformation functions are complicated, involving all variables in a sensitive way. A small variation of any one (variable) changes the outputs considerably.” This implied that small changes may result into large changes and if this be mapped to chaos theory it will mean that chaotic behavior will continue to manifest the effects of any minuscule disturbances. However, it is to be noted that systems used in chaos are defined on real numbers only (Gickenheimer & Holmes, 1983) whereas cryptographic systems operate on finite number of integers (Schneier, 1996). The two disciplines can form a symbiotic relationship in cryptography which is explained by the works of many researchers in the following paragraph.
Related Content

Designing a Secure Cloud Architecture: The SeCA Model
[www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a](www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a)

Password Sharing and How to Reduce It
[www.igi-global.com/chapter/password-sharing-reduce/46886?camid=4v1a](www.igi-global.com/chapter/password-sharing-reduce/46886?camid=4v1a)

A Reliable Data Provenance and Privacy Preservation Architecture for Business-Driven Cyber-Physical Systems Using Blockchain

(R)Evolutionary Emergency Planning: Adding Resilience through Continuous Review
[www.igi-global.com/article/revolutionary-emergency-planning/152163?camid=4v1a](www.igi-global.com/article/revolutionary-emergency-planning/152163?camid=4v1a)