Preface

The Book

This book is an intersection of two major subject area, chaos synchronization and cryptography.

Chaos theory has a huge applicability in different branches of Science, Engineering and Management. It is highly important in physical, biological, social Sciences for its unique capability to model the natural systems which are nonlinear. In the field of engineering, chaos is very useful for control theory and applications. Genetic engineering algorithms, Swarm Intelligence, different global optimization techniques are useful in engineering and also in management for economic research and stock predictions.

Synchronization is a special phenomenon of chaotic systems. Two system can synchronize when they are both chaotic in nature. This phenomenon has wide applications in neural network and cryptography.

The content of the book is recent developments of the subject area.

Organization of the Book

The book is divided in three sections. The first section contains five chapters describing the dynamics of different chaotic systems with theory, simulations and experiments. Section 2 is based on nine chapters on synchronization of chaotic systems. The phenomenon have investigated with chaotic oscillators, integer and fraction order systems and delayed neural networks. Section 3 contains seven chapters based on cryptographic applications of chaotic systems.

Chapter 1: “Dynamical Systems and their Chaotic Properties” Konstantinos Chlouverakis presents an analytical observation on ordinary and time delayed dynamical systems and there chaotic properties. The non linearity have quantified with phase space diagrams, lyapunov exponents, bifurcation diagrams. The stability analysis is also computed and a coupled system is also studied for cryptographic encoding.

Chapter 2: “Chaotic Dynamical Systems Associated with Tilings of $\mathbb{R}^N$” Lionel Rosier presents a mathematical mechanism for chaos synchronization that can be applied to encryption. A class of discrete dynamical systems is defined on the homogeneous space associated with a regular tiling of $\mathbb{R}^N$ because any dynamical system in this class is chaotic in the sense of Devaney, and that it admits at least one positive Lyapunov exponent. A common example of such a system is the $N$-dimensional torus $T^N$.

Chapter 3: “Identification and State Observation of Uncertain Chaotic Systems Using Projectional Differential Neural Networks” Alejandro Garcia, Isaac Chairez and Alexander Poznyak made an approximation of dynamical systems by artificial neural networks and studied the analysis of projectional differential neural network. The effectiveness of the novel DNN topology is shown by a classical numerical example of Chua’s circuit.
Chapter 4: “Simple Chaotic Electronic Circuits” M.P. Hanias and G.S. Tombras considers that simple chaotic electronics circuits in the form of diode resonator circuits, Resistor-Inductor-LED optoelectronic chaotic circuits and Single Transistor chaotic circuits can be used as transmitters and receivers for chaotic cryptosystems. These circuits are flexible to the changes in their circuit parameters and so help in investigating the influence of such changes in complexity of the generated strange attractors. The authors have performed a time series analysis based on Grassberger and Procaccia’s method. The invariant parameters such as correlation, and minimum embedding dimension are respectively calculated along with the Kolmogorov entropy. The chapter also examines the RLT circuits when they are in a critical state.

Chapter 5: “Experimental Evidences of Shil’nikov Chaos and Mixed-Mode Oscillation in Chua Circuit” Syamal Kumar Dana and Satyabrata Chakraborty in their chapter have provided the evidence of Shil’nikov type homoclinic chaos in asymmetry-induced Chua’s oscillator. In the experiment, different time scales are artificially created in a double scroll Chua attractor by inducing asymmetry in the system by external DC forcing. One of the double scroll attractors shrinks in size and creates an additional time scales in the overall dynamics that plays a crucial role in the origin of homoclinic chaos, bursting and MMOs.

Chapter 6: “Synchronization of Chaotic Oscillators” J. M. González-Miranda presents a review about the varied forms which the mutually coupled or unidirectionally driven dynamic chaotic oscillators display on synchronization. This will enlighten the readers on the key role which physics and mathematics play in laying the foundation useful for reaping the benefits of chaos synchronization in telecommunications and cryptography.

Chapter 7: “Synchronization in Integer and Fractional Order Chaotic Systems” Ahmed E. Matouk’s, chapter concentrates on the synchronization techniques on integer and fractional order chaotic systems. Lyapunov stable theory are also used to control the synchronized error. Numerical examples well support the analytical results.

Chapter 8: “Chaos Synchronization” Hassan Salarieh and Mohammad Shahrokhi investigates an overview of the synchronization phenomenon in secure communication. The chapter begins by defining complete, lag, phase and generalized synchronization approaches followed by the application of control theory for synchronization of different chaotic systems. They have presented some synchronization algorithms based on different control techniques. They have shown ways to modify the controlling methods in order to cope with parameter uncertainties and measurement noise. The performance of the discussed methods are supported by simulation of several chaotic systems.

Chapter 9: “Chaotic Gyros Synchronization” In this Chapter, M. Roopaei, M. J. Zolghadri, B. S. Ranjbar, S. H. Mousavi, H. Adloo, B. Zare and T.C. Lin have presented three methods for synchronizing of two chaotic gyros in the presence of uncertainties, external disturbances and dead-zone nonlinearity. In the first method, there is dead-zone nonlinearity in the control input, which limits the performance of accurate control methods. The effects of this nonlinearity have been attenuated using a fuzzy parameters adaptation integrated with sliding mode control method. For the second method, they have proposed a robust adaptive fuzzy sliding mode control scheme to overcome the synchronization problem for a class of unknown nonlinear chaotic gyro. The third method considers two different gyro systems. For this method they also have proposed a fuzzy controller to eliminate chattering phenomena during the reaching phase of sliding mode control. All the mentioned methods are simulated and the results illustrate the effectiveness of the proposed methods.

Chapter 10: “Importance of Chaos Synchronization on Technology and Science” In this chapter, Ricardo Aguilar-López, Ricardo Femat and Rafael Martínez-Guerra highlight the importance of chaos
synchronization on technology and science. The chapter introduces their attempt in three sections. The first sections deals with the topic of synchronized state in the sense of identical synchronization. This is realized with the robust nonlinear observer design, considering corrupted measurements and model uncertainties, coupling uncertainty estimators with nonlinear state observers. In the second part of their chapter, the authors have addressed applications to chaos communications primarily an application of chaos theory which is aimed to provide security in the transmission of information performed through telecommunications technologies mainly dealing with the transmitter. A message is added on to a chaotic signal and then, the message is masked in the chaotic signal. When the chaotic signal carries such a message it is called the chaotic carrier. All this is done via control theory and is a particular case of chaos synchronization. In the last section they have discussed an application to synchronization of biological systems. Their attempt of introducing the feedback control laws in some biological systems is influenced by the behavior of biophysical mechanisms of cellular dynamics. The authors also present links between feedback control schemes, with an external input, and intracellular calcium functions for coordination and control.

**Chapter 11:** “Synchronization of Oscillators” Jean B. Chabi Orou describes the synchronization of oscillators in a lucid manner which can facilitate to get a grasp of the main concepts before delving into the different kinds of synchronization configurations, Chaotic synchronization and also addressed the issue of stability of the synchronization. They have briefly mentioned the influence of noise on the synchronization process.

**Chapter 12:** “Synchronization of Uncertain Neural Networks with $H_{\infty}$ Performance and Mixed Time-Delays” Hamid Reza Karimi, introduces an exponential synchronization method for a class of uncertain master and slave neural networks with mixed time-delays. The mixed delays comprise different neutral, discrete and distributed time-delays. In order to design a delayed state-feedback control as a synchronization law in terms of linear matrix inequalities under less restrictive conditions, some delay-dependent sufficient conditions have been established by an appropriate discretized Lyapunov-Krasovskii functional and some free weighting matrices. Irrespective of their initial state, this controller will guarantee the exponential synchronization of the two coupled master and slave neural networks. The author has demonstrated the effectiveness of the established synchronization laws by suitable numerical simulations.

**Chapter 13:** “Adaptive Synchronization in Unknown Stochastic Chaotic Neural Networks with Mixed Time-Varying Delays” Jian-an Fang and Yang Tang investigate the problem of synchronization and parameter identification for a class of chaotic neural networks. The author identifies the importance of the inherent features of high security of neural networks and their potential in applications such as pattern recognition, image processing to name a few. These features have aroused interest in synchronization of chaotic neural network (CNN). They have carried out their work with stochastic perturbation via state and output coupling, which involve both the discrete and distributed time-varying delays. They have derived several sufficient conditions in order to perform synchronization of stochastic chaotic neural networks with the help of adaptive feedback techniques. They claim to estimate all the connection weight matrices when the lag synchronization and complete synchronization is achieved in mean square at the same time. They have supported the effectiveness of their proposed method with suitable simulation.

**Chapter 14:** “Type-2 Fuzzy Sliding Mode Synchronization” Tsung-Chih Lin, Ming-Che Chen, Mehdi Roopaei presents an adaptive interval type-2 fuzzy neural network (FNN) controller to synchronize chaotic systems with training data corrupted by noise or rule uncertainties involving external disturbances. The scheme is applied for the synchronization of non-identical chaotic systems. The asymptotic stability is also studied by the Lyapunov stability theorem. The simulation results prove the effectiveness of the scheme.
**Chapter 15:** “Secure Transmission of Analog Information using Chaos” A.S. Dmitriev, E.V. Efremova, L.V. Kuzmin, A.N. Miliou, A.I. Panas, S.O. Starkov present an experimental study of a practical realization of a complex analog signal transmission system using dynamic chaos. They attempt to use the synchronized chaotic system for secure wireless communications in RF band. An analysis of the restrictions and problems connected with the quality of synchronization of the transmitter and the receiver of the wireless communication systems has also been demonstrated. In wireless transmission various perturbing factors degrade its quality and the primary reason for this can be attributed to the chaotic response desynchronization associated with the phenomenon of “on-off” intermittency. Their investigation reveals that the quality of transmission can be improvised on increasing the level of information signal fed to the transmitter. On the other hand, for secure communication the information signal level must be reduced. Hence, they claim that if a compromise be made on these contradictory requirements then an improvement of the quality of the synchronous chaotic response in the receiver can be achieved.

**Chapter 16:** “Control-Theoretical Concepts in the Design of Symmetric Cryptosystems” Gilles Millérioux and José Maria Amigó in this chapter focus on the fact that message-embedded chaotic ciphers and conventional self-synchronizing stream ciphers are equivalent under the so-called flatness condition. The flatness condition is borrowed from control theory. The authors claim that this kind of chaotic cipher may be an interesting alternative for the design of Self-Synchronizing Stream Ciphers and suggest new approaches in the design of self-synchronizing stream ciphers. This chapter focusses on digital encryption and hence on discrete-time dynamical systems/maps. The authors highlight the state-of-the-art of the structures involved in chaotic cryptographic schemes in comparison to conventional ciphers especially with symmetric ciphers. The initial sections are dedicated on the background of cryptography and its different modes with significance to stream ciphers with explanation of ways of deriving some permutation or substitution ciphers from chaotic dynamical systems for cryptographic purposes, followed by reviews of popular synchronization-based cryptosystems and outlining important issues to be addressed.

**Chapter 17:** “Unmasking Optical Chaotic Cryptosystems Based on Delayed Optoelectronic Feedback” Silvia Ortín, Luis Pesquera presents an analysis of the security of optical chaotic communication systems. Their result shows that such chaotic cryptosystems based on feedback with several fixed time delays are vulnerable to security hazards. To achieve this they have developed a model based on a new type of neural network known as modular neural network. This model reconstructs the nonlinear dynamics of the transmitter from experimental time series in the single-delay case and also from numerical simulations in single and two-delay cases. To support their experiment they have generated the chaotic carrier by a laser diode when it is subjected to delayed optoelectronic feedback. The authors have demonstrated that even if the chaotic attractor manifests itself in huge dynamics, the model’s complexity does not increase (remains unaffected ?) on increasing the time delay. Whereas, the reconstruction of nonlinear dynamics is more difficult when the feedback strength is increased. The developed model is utilized as an unauthorized receiver which recovers the message.

**Chapter 18:** “Encryption of Analog and Digital Signals through Synchronized Chaotic Systems” Kehui Sun has analyzed the basic principles of chaos based communication tools in cryptography in analogue and digital medium mainly Chaos Masking, Chaos Shift Keying, Chaos Modulation, and Chaos Spreading Spectrum. The author has also analyzed their modifications and performances of chaotic sequence supported by appropriate simulation tools and designed an effective chaotic sequence generator. This has been used in their proposed two encryption schemes namely chaotic sequence encryption and chaotic data stream encryption.
Chapter 19: “Digital Information Transmission using Discrete Chaotic Signal” A.N. Anagnostopoulos, A.N. Miliou, S.G. Stavrinides, A.S. Dmitriev and E.V. Efremova have studied a digital information transmission system using discrete chaotic signal over cable and proposed a robust, secure approach of transmission with an enhanced encoding scheme to inject further security. This has been designed keeping in mind the simplicity factor of implementing a chaotic system for the purpose. To realize the aim, the authors have used a non-autonomous 2nd order non-linear oscillator system presented in (Tamaševičius, Čenys, Mycolaitis, & Namajunas, 1998) supported with results on synchronization. The authors also analyze the effect of noise (internal or external) on the synchronization of the drive-response system (unidirectional coupling between two identical systems). They have also taken into account the practical issue pertaining to the mismatch between the parameters of the transmitter and the receiver resulting due to different operating conditions of the otherwise identical transmitter and receiver circuits.

Chapter 20: “Mathematical Treatment for Constructing a Countermeasure Against the One Time Pad Attack on the Baptista Type Cryptosystem.” M.R.K. Ariffin and M.S.M. Noorani present a notion for preventing a one time pad attack on the chaotic cryptosystem proposed by M.S. Baptista in 1998. They have discussed the weakness of this cryptosystem to be its vulnerability to one-time pad attack (a type of chosen plaintext attack) together with the non-uniform distribution of ciphertexts. Hence, the authors have given a mathematical approach with an example to show the Baptista type cryptosystem can be prevented against the one-time pad attack.

Chapter 21: “Chaos Synchronization with Genetic Engineering Algorithm for Secure Communications.” Sumona Mukhopadhyay Mala Mitra and Santo Banerjee have proposed a method of digital cryptography inspired from Genetic Algorithm (GA) and synchronization of chaotic delayed system. The chapter introduces a brief idea about the concept of Evolutionary Algorithm (EA) and demonstrates how the potential of dynamical system such as chaos and EA can be utilized in a reliable, efficient and computational cheaper method for secure communication. GA is a subclass of Evolutionary algorithm and as such is governed by the rules of organic evolution. In GA the selection mechanism and both transformation operators—crossover and mutation are probabilistic. The parameters and the keys are secure since the synchronized dynamical system does not necessitate the transmission of keys over the communication channel. The random sequence obtained from chaotic generator further transforms it into a powerful stochastic method of searching the solution space in varied directions for an optimal solution escaping points of local optima. But randomicity can sometimes destabilize the system and there is no guarantee that it yields an improved solution. The authors substituted the random and probabilistic selection operator of GA with problem specific operator to design the cryptosystem to control such random behavior otherwise it would lead to a solution which is uncorrelated with the original message and may also lead to loss of information. The way selection has been modified leads to two versions of the proposed genetic engineering algorithm for cryptography. Simulation results demonstrates that both the flavors of the proposed cryptography successfully recover the message and a comparison with cryptography with $(\mu,\rho,\lambda)$ Evolutionary Strategy’s selection scheme shows a computational edge of their proposed work.

Intended Audience

This book can be used as a reference for the scientific and industrial research. The different chapters can provide knowledge of the subject areas, as well as the developments in the field of theory and applications. The science and engineering students will be benefited to learn the subject by some review chapters, also they have the scope to continue some developments with the existing and new research work described here.