Studies in Computational Intelligence, Volume 354

Editor-in-Chief
Prof. Janusz Kacprzyk
Systems Research Institute
Polish Academy of Sciences
ul. Newelska 6
01-447 Warsaw
Poland
E-mail: kacprzyk@ibspan.waw.pl

Further volumes of this series can be found on our homepage: springer.com

Vol. 330. Steffen Rendle
Context-Aware Ranking with Factorization Models, 2010
ISBN 978-3-642-16897-0

Vol. 331. Athena Vakali and Lakhmi C. Jain (Eds.)
New Directions in Web Data Management 1, 2011
ISBN 978-3-642-17550-3

Vol. 332. Jianguo Zhang, Ling Shao, Lei Zhang, and Graeme A. Jones (Eds.)
Intelligent Video Event Analysis and Understanding, 2011
ISBN 978-3-642-17553-4

Vol. 333. Fedja Hadzic, Henry Tan, and Tharam S. Dillon
Mining of Data with Complex Structures, 2011
ISBN 978-3-642-17556-5

Vol. 334. Álvaro Herrero and Emilio Corchado (Eds.)
Mobile Hybrid Intrusion Detection, 2011
ISBN 978-3-642-18298-3

Vol. 335. Radomir S. Stankovic and Radomir S. Stankovic
From Boolean Logic to Switching Circuits and Automata, 2011
ISBN 978-3-642-11681-0

Vol. 336. Paolo Remagnino, Dorothy N. Monekosso, and Lakhmi C. Jain (Eds.)
Innovations in Defence Support Systems – 3, 2011
ISBN 978-3-642-18277-8

Vol. 337. Sheryl Brahnam and Lakhmi C. Jain (Eds.)
Advanced Computational Intelligence Paradigms in Healthcare 6, 2011
ISBN 978-3-642-17823-8

Vol. 338. Lakhmi C. Jain, Eugene V. Aidman, and Canicious Abeynayake (Eds.)
Innovations in Defence Support Systems – 2, 2011
ISBN 978-3-642-17763-7

Vol. 339. Halina Kwasnicka, Lakhmi C. Jain (Eds.)
Innovations in Intelligent Image Analysis, 2010
ISBN 978-3-642-17933-4

Vol. 340. Heinrich Hussmann, Gerrit Meixner, and Detlef Zuehlke (Eds.)
Model-Driven Development of Advanced User Interfaces, 2011
ISBN 978-3-642-14561-2

Vol. 341. Stéphane Doncieux, Nicolas Bredeche, and Jean-Baptiste Mouret(Eds.)
New Horizons in Evolutionary Robotics, 2011
ISBN 978-3-642-18271-6

Vol. 342. Federico Montesino Pouzols, Diego R. Lopez, and Angel Barriga Barros
Mining and Control of Network Traffic by Computational Intelligence, 2011
ISBN 978-3-642-18083-5

Vol. 343. Kurosh Madani, António Dourado Correia, Agostinho Rosa, and Joaquim Filipe (Eds.)
Computational Intelligence, 2011
ISBN 978-3-642-20205-6

Vol. 344. Atilla Elçi, Mamadou Tadiou Koné, and Mehmet A. Orgun (Eds.)
Semantic Agent Systems, 2011
ISBN 978-3-642-18307-2

Vol. 345. Shi Yu, Léon-Charles Tranchevent, Bart De Moor, and Yves Moreau
Kernel-based Data Fusion for Machine Learning, 2011
ISBN 978-3-642-19405-4

Vol. 346. Weisi Lin, Dacheng Tao, Janusz Kacprzyk, Zhu Li, Ebroul Izquierdo, and Haohong Wang (Eds.)
Multimedia Analysis, Processing and Communications, 2011
ISBN 978-3-642-19550-1

Vol. 347. Sven Helmer, Alexandra Poulovassilis, and Fatos Xhafa
Reasoning in Event-Based Distributed Systems, 2011
ISBN 978-3-642-19723-9

Vol. 348. Beniamino Murgante, Giuseppe Borruso, and Alessandra Lapucci (Eds.)
Geocomputation, Sustainability and Environmental Planning, 2011
ISBN 978-3-642-19732-1

Vol. 349. Vitor R. Carvalho
Modeling Intention in Email, 2011
ISBN 978-3-642-19955-4

Vol. 350. Thanasis Daradoumis, Santi Caballé, Angel A. Juan, and Fatos Xhafa (Eds.)
Technology-Enhanced Systems and Tools for Collaborative Learning Scaffolding, 2011
ISBN 978-3-642-19813-7

Vol. 351. Ngoc Thanh Nguyen, Bogdan Trawiński, and Jason J. Jung (Eds.)
New Challenges for Intelligent Information and Database Systems, 2011
ISBN 978-3-642-19952-3

Vol. 352. Nik Bessis and Fatos Xhafa (Eds.)
Next Generation Data Technologies for Collective Computational Intelligence, 2011
ISBN 978-3-642-20343-5

Vol. 353. Igor Aizenberg
Complex-Valued Neural Networks with Multi-Valued Neurons, 2011
ISBN 978-3-642-20352-7

Vol. 354. Ljupco Kocarev and Shiguo Lian (Eds.)
Chaos-Based Cryptography, 2011
ISBN 978-3-642-20541-5

Ljupco Kocarev and Shiguo Lian (Eds.)

Chaos-Based Cryptography

Theory, Algorithms and Applications

Springer

Prof. Ljupco Kocarev
Macedonain Academy of Sciences and Arts
bul. Krste Misirkov 2, P.O. Box 428
1000 Skopje, Republic of Macedonia
E-mail: lkocarev@manu.edu.mk,
lkocarev@ucsd.edu

Dr. Shiguo Lian
France Telecom R&D Beijing
2 Science Institute South Rd, Haidian District
Beijing, 100080, China
E-mail: shiguo.lian@orange-ftgroup.com

ISBN 978-3-642-20541-5 e-ISBN 978-3-642-20542-2

DOI 10.1007/978-3-642-20542-2

Studies in Computational Intelligence ISSN 1860-949X

Library of Congress Control Number: 2011926008

Typeset & *Cover Design:* Scientific Publishing Services Pvt. Ltd., Chennai, India.

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Preface

Chaos is an interesting phenomenon that often happens in some systems in various fields, e.g., physics, psychology, biology, etc. Chaos theory provides the means to explain chaos phenomenon, control chaotic dynamic systems and make use of chaos properties. Now, chaos has been used in physics, chemistry, neurophysiology, engineering, etc. Especially, chaos' properties, such as randomness and ergodicity, have been proved to be suitable for designing the means for data protection. During the past decade, many chaos-based cryptographic techniques have been studied, such as the chaos-based secret communication, chaos-based block/stream cipher, chaos-based random number generation, chaos-based hash, etc. Additionally, some secure applications based on chaos have been investigated, e.g., chaos-based image encryption or authentication, video/audio scrambling, multimedia copyright protection, etc.

To the best of our knowledge, this is the first book edited on chaos applications in cryptography. Chaos-based cryptography is a new research field across two fields, i.e., chaos (nonlinear dynamic system) and cryptography (computer and data security). To access the latest research related to chaos applications in cryptography, we launched the book project where researchers from all over the world provide the necessary coverage of the mentioned field. The primary objective of this project was to assemble as much research coverage as possible related to the field by defining the latest innovative technologies and providing the most comprehensive list of research references.

The book includes eleven chapters highlighting current concepts, issues and emerging technologies. Distinguished scholars from many prominent research institutions around the world contribute to the book. The book covers various aspects, including not only some fundamental knowledge and key techniques, but also typical applications and open issues. For example, the following topics are investigated in detail: fundamentals of chaos, relation between chaos and cryptography, Pseudo-Random Number Generation (PRNG) based on digitized chaos, cipher design based on high-dimensional chaotic maps, chaos-based hash function, and chaos-based video encryption. Additionally, the cryptanalysis of chaotic cipher and the corresponding lessons are presented in a thorough manner. Finally, some hardware implementations of chaotic ciphers and the performance evaluation compared with traditional ciphers are proposed in deep. For each of the topics, both the latest research results and open issues or hot topics are reviewed and analyzed.

The diverse and comprehensive coverage of multiple disciplines in the field of chaos based cryptography will contribute to a better understanding of all topics, research, and discoveries in this emerging and evolving field. Furthermore, the contributions included in this book will be instrumental in the expansion of the body of knowledge in this field. The coverage of this book provides strength to this reference resource for both researchers and also decision makers in obtaining a greater understanding of the concepts, issues, problems, trends, challenges and opportunities related to this field of study. It is our sincere hope that this publication and its great amount of information and research will assist our research colleagues, all faculties, their students, and our organizational decision makers in enhancing their understanding of this research field. Perhaps this publication will even inspire its readers to contribute to the current discoveries in this immense field.

Editors

Prof. Ljupco Kocarev
University of California, USA

Dr. Shiguo Lian
France Telecom R&D (Orange Labs) Beijing, China

Acknowledgments

The editors would like to acknowledge the help of all involved in the collation process of the book, without whose support the project could not have been satisfactorily completed. Deep appreciation and gratitude is due to the authors of chapters, whose efforts make the high-quality project.

Special thanks go to the publishing team at Springer, whose contributions throughout the whole process from inception of the initial idea to final publication have been invaluable. In particular to Dr. Thomas Ditzinger, who continuously prodded via e-mail for keeping the project on schedule and to other editors who help to make the book publishable.

And last but not least, our families, for their unfailing support and encouragement during the months it took to give birth to this book.

February 2011 Editors

Contents