Preface

The global economic infrastructure is becoming increasingly dependent upon information technology, with computer and communication technology being essential and vital components of Government facilities, power plant systems, medical infrastructures, financial centers and military installations to name a few. Finding effective ways to protect information systems, networks and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals.

This volume provides the academic and industrial community with a medium for presenting original research and applications related to information assurance and security using computational intelligence techniques. The included chapters communicate current research on information assurance and security regarding both the theoretical and methodological aspects, as well as various applications in solving real world information security problems using computational intelligence.

In Chapter 1, which is entitled *Cryptography and Cryptanalysis Through Computational Intelligence*, the authors give a brief introduction to cryptography and Computational Intelligence methods, followed by a short survey of the applications of Computational Intelligence to cryptographic problems. Their contribution in this field is presented. Specifically, some cryptographic problems are viewed as discrete optimization tasks and Evolutionary Computation methods are utilized to address them. The authors show that Artificial Neural Networks are effective in approximating some cryptographic functions. They also present some theoretical issues of Ridge Polynomial Networks and cryptography.

In Chapter 2, which is entitled *Multimedia Content Protection Based on Chaotic Neural Networks*, the author gives a brief introduction to chaotic neural network based data encryption, including stream ciphers, block ciphers and hash functions. Then, he analyzes chaotic neural networks' properties that are suitable for data encryption, such as parameter sensitivity, random

similarity, diffusion property, confusion property, one-way property, etc. The author also gives some proposals to design chaotic neural network based cipher or hash function, and uses these ciphers to construct media encryption and authentication methods.

In Chapter 3, which is entitled *Evolutionary Regular Substitution Boxes for Secure Cryptography Using Nash equilibrium*, the authors focus on engineering regular Substitution Boxes or S-boxes that present high non-linearity and low auto-correlation properties using evolutionary computation. There are three properties that need to be optimised: regularity, non-linearity and auto-correlation. The authors exploit the Nash equilibrium-based multi-objective evolutionary algorithm to engineer resilient substitution boxes.

In Chapter 4, which is entitled *Industrial Applications Using Wavelet Packets for Gross Error Detection*, the authors address the Gross Error Detection using uni-variate signal-based approaches and propose an algorithm for the peak noise level determination in measured signals. More specifically, they present developed algorithms and results using two uni-variate, signal-based approaches regarding performance, parameterization, commissioning, and on-line applicability. They base their approach on two algorithms: the Median Absolute Deviation (MAD) a nd the wavelet-based one. Many findings are drawn form the comparison.

In Chapter 5, which is entitled *Immune-inspired Algorithm for Anomaly Detection*, the author presents a new theory: the Danger theory and Dendritic cells, and explores the relevance of those to the application domain of security. He introduces an immune based anomaly detection approach from the abstraction of Danger theory. He also presents the derivation of bio-inspired anomaly detection from the DC functionality with Danger theory, and depicts two examples of how the proposed approach can be applied for computer and network security issues with preliminary results.

In Chapter 6, which is entitled *How to Efficiently Process Uncertainty within a Cyberinfrastructure*, the authors propose a simple solution to the problem of estimating uncertainty of the results of applying a black-box algorithm – without sacrificing privacy and confidentiality of the algorithm.

In Chapter 7, which is entitled *Fingerprint Recognition Using a Hierarchical Approach*, the authors introduce a topology-based approach to fingerprint recognition utilizing both global and local fingerprint features. They also describe a new hierarchical approach to fingerprint matching which can be used to accelerate the speed of fingerprint identification in large databases. Furthermore, the authors propose to apply Radial Basis Functions to model fingerprint's elastic deformation, which greatly increases the system's tolerance to distorted images. They claim that experimental results confirm that the proposed hierarchical matching algorithm achieves very good performance with respect to both speed and accuracy.

In Chapter 8, which is entitled *Smart Card Security*, the authors describe the various attacks that can be applied to smart cards, and the subsequent countermeasures required in software to achieve a secure solution. A case

study on the various generations of the European mobile telephone networks is given as an example of how the deployment of countermeasures has changed due to the described attacks.

In Chapter 9, which is entitled *Governance of Information Security: New Paradigm of Security Management*, the author provides a structured approach of security governance to corporate executives. He summarises previous studies on the governance and security management to be able to explain the components and requirements of a governance framework for corporate security. The author provides a governance framework for corporate security, which consists of four domains and two relationship categories.

We are very much grateful to the authors of this volume and to the reviewers for their tremendous service by critically reviewing the chapters. The editors would like also to thank Prof. Janusz Kacprzyk, the editor-in-chief of the Studies in Computational Intelligence Book Series and Dr. Thomas Ditzinger, Springer Verlag, Germany for the editorial assistance and excellent cooperative collaboration to produce this important scientific work. We hope that the reader will share our excitement to present this volume on **Computational Intelligence in Information Assurance and Security** and will find it useful.

November 2006

Nadia Nedjah[1], **Ajith Abraham**[2] and **Luiza M. Mourelle**[1] (Eds.)

[1]State University of Rio de Janeiro, Brazil
[2]IITA Professorship Program, Chung-Ang University, Korea

http://www.springer.com/978-3-540-71077-6

Computational Intelligence in Information Assurance and Security
Abraham, A. (Ed.)
2007, XX, 255 p., Hardcover
ISBN: 978-3-540-71077-6