Preface

The explosive growth in computer systems and their interconnections via networks has increased the dependence of organizations on the information stored and communicated using these systems. With the increasing degree of sophistication and evolution of threats, it becomes crucial to propose and explore novel methodologies to protect data and systems confidentiality, integrity and availability. Several innovative ideas have been proposed including computational intelligence (CI) paradigms due to their very attractive inherent characteristics including adaptation, self-organization, parallelizability, computational efficiency, fault tolerance and error resilience. These paradigms are widely recognized as a significant source of competitive advantage by many authors.

Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, modification, or disruption. It is the protection of information and its elements, including the systems and hardware that use, store, and transmit that information.

To protect stored, processed, and transmitted information, there are different mechanisms. Security mechanisms are the means for implementing security services. They can be divided into three broad categories: Prevention, Detection, and Recovery.

One of these mechanism is encryption. Any cryptographic system (cryptosystem, or cipher system) has five elements: plaintext (clear text), ciphertext (encrypted text), encryption algorithm which is a procedure used to encipher (encrypt) the plaintext and transform it to ciphertext. Decryption algorithm which is the inverse of the encryption algorithm, and the key which is a parameter used to prevent the plaintext from being easily revealed by an authorized person. A number of cryptosystems for encrypting the private information have been proposed which are of different levels of security; these cryptosystems can be classified into modern and classical systems. The basic building blocks of all cryptosystems are substitution and transposition.

Cryptography is the study of encryption techniques for protecting information, and also the techniques used to attack encryption techniques. Thus it is combination of two areas: cryptanalysis and cryptography.

We have other security mechanisms, such as entity authentication, digital signature, and information hiding. Steganography is an art and science of hiding information within other information. Entity authentication is a technique designed to let one party prove the identity of another party. By using the digital signature, the sender uses a signing algorithm to sign the message, then the message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted; otherwise, it is rejected.
On the other hand, there are a number of CI techniques can be used in information security. Genetic algorithm (GA) is a search algorithm based on the mechanics of natural selection and natural genetic. GA attempts to identify optimal solution by applying the techniques of natural selection to a population of solutions, the solutions are evaluated, the bad solutions are killed, and the remaining solution are recombined (mate) to form a new generation of solution.

Genetic programming (GP) is an application of GA, in which the structure under adaption is a set of computer programs. It is capable of evolving computer program that solve, or approximately solve, a variety of problem. Thus, GP individual is designed to store computer programs in such a way that they can be optimized using an evolutionary approach.

Cryptology problems, such as designing good cryptographic systems and analyzing them, attract many researchers, and hence we can find in the literatures different techniques and methods that have been proposed to solve these problems. In recent years, many algorithms that take advantage of approaches based on computational intelligence techniques (such as genetic algorithms, genetic programming, etc.) have been proposed.

In this proposed edited book, the most important achievements in solving security problems using CI techniques such as GA and GP are presented. The main objective is to show the applicability of these techniques in solving these problems, in addition to give interested researchers an overview of the new methodologies and new directions in information security.

The proposed book is to create an integrated and coherent book of the applications of CI and other advanced techniques in information security which will add value to the current research, and which will contribute to a better understanding of the factors that influence successful security systems design in security industry.

Moreover, it will encourage the security industry to take a proactive attitude toward CI techniques; thus resulting in a better design of security systems. Hence, publishing this book will be of interest to researchers, academics, students and practitioners of information security.

Very few studies have been conducted into the applications of CI techniques in information security. The proposed book will therefore contribute and add to the current research in information technology; furthermore, this book will instigate several opportunities for future research.

The book will have implications for information security in general, and specifically for practitioners. Firstly, this study will expand on the current understanding of CI techniques by exploring and investigating various factors and how they relate to the success of security systems design. A number of methods will be applied, in order to overcome the elements that are missing in the current research, and particular focus will be placed on testing the effectiveness of CI techniques.

There is little research that examines the effectiveness of CI on security industry; this book will therefore examine its impact, furthermore, it will determine the most effective way of designing and attacking security systems.

The prospective audience for this book will be researchers, academics and practitioners from the following fields of research: computational intelligence, information security, security engineering.

This book will increase information security awareness in organizations by providing a clear direction for the effective implementation of information security and CI, which could improve organizational learning and performance excellence. The book covers the most important concepts and key issues which relate CI to information security, and also cover emerging practices in information security. This book also aims to increase CI awareness in information security by providing a clear direction for the
effective implementation of CI techniques which would improve information security industry. In this sense, the intended audience will include all researchers who are trying to find effective methods for designing and attacking security systems.

On the other hand, computational intelligence (CI) and information security has become an agenda issue in various academic and professional journals. It has become recognized as a significant source of competitive advantage by many authors.

Although the applications of CI (and other advanced techniques) in information security has been widely discussed by many academicians and practitioners, there is no specific book to discuss and provide information on how we can apply the CI techniques to solve the problems of information security.

The book is organized into ten chapters. A brief description of each of the chapters follows:

Chapter 1 provides a detailed introduction to major CI paradigms. It includes a discussion of Neural Networks (NN) which is an important area of CI mainly inspired by the biological system of neurons in human brain, and Evolutionary Computation (EC) which is inspired by the evolution of biological objects. Furthermore, it presents Swarm Intelligence (SI), Fuzzy Systems (FS), and Hybrid Systems (HS). It also shades the light on some of potential applications in information security and cryptography.

Chapter 2 demonstrates how CI has attracted the attention of many researchers for its effectiveness in solving different kinds of problems in cryptology. The chapter aims at demonstrating the applicability of CI in cryptology and presenting an overview of existing applications of CI in cryptology. The problems examined in this chapter are the automated design of cipher systems, and the automated cryptanalysis of cipher systems. It has been shown that CI methods, such as genetic algorithm and genetic programming, can be effective tools to solve many cryptology problems.

Chapter 3 proposes a new effective algorithm to design stream cipher systems automatically using simulated annealing and genetic programming with a different representation method for the population individuals. In the proposed method, the candidate programs (population individuals) are represented as strings of integers representing the individual program syntactic rule numbers. Genetic programming with this representation method is called genetic algorithm for developing software (GADS). The performance of the proposed algorithm is evaluated by applying different genetic methods and parameters. Finally, the proposed method is compared with other representation methods such as LISP expressions.

Chapter 4 shows how important it is to protect sensitive data in many personal, commercial, governmental, medical and military applications. The chapter provides an approach for data encryption in cyber security by storing and communicating data in unintelligible form. It provides a review of the work related to image cryptosystems based on chaos theory and biologically-inspired algorithms. Then, a case study is presented using ideas from genetic crossover and mutation to confuse and diffuse images to generate secure cipher images with very low correlation between pixels.

Chapter 5 illustrates the work in the field of security and its impact on ascertainment of innovative ideas along with their practical applicability. It explains that adequate remedies are not accomplished yet due to the enhanced technological aspects even in the unlawful communities and how they become a major concern for the security agencies and can be considered as unaddressed issue. The chapter provides an introduction to Intrusion Detection Systems (IDSs) and explains how IDS is a means for detecting the intrusive events concealed among the activities of normal users. Additionally, such systems also provide necessary assistance in preventing future intrusions. The present chapter focuses on improving the performance of the IDS in order to meet the contemporary progression by proposing a system which is effective, adaptive and intelligent in nature and is able to remarkably detect intrusions. In order to accomplish the desired system, the chapter involves development of intelligent IDS.
Chapter 6 starts by explaining how Mobile Ad-hoc NETworks (MANETs) are believed to be highly vulnerable to security threats due to the numerous constraints they present such as: the absence of a fixed infrastructure, the dynamic topology change, their dependence on cooperative communication, the unreliability of wireless links, and most importantly the absence of a clear line of defense. The chapter illustrates the approaches to utilize agent technology to build optimal, adaptive and comprehensive intrusion detection systems to fit MANET security requirements. It presents a survey and analyzes the work that has been recently done for the deployment of agent technology in the area of MANET intrusion detection. In particular, recent advances in that field in terms of existing frameworks, architectures and implementations as well as a discussion of the obtained advantages in addition to the potentially introduced vulnerabilities are presented.

Chapter 7 aims to describe the applications of Digital Signature Certificates for Online Information Security. The chapter discusses online information security through cryptography. It explains and illustrates digital signature certificates; their benefits, underlying standards, involved techniques, procedures, algorithms, processes, structure, management, and formats. It highlights the potential of digital signatures and certificates in information security across different devices, services, and applications. It introduces a few useful tools to learn, train, and implement digital signature certificates. Further, it illustrates systematic procedures for securing documents and e-mail messages through digital signature certificates.

Chapter 8 shows how cryptomodules can increase security of wireless sensor network and possibilities of biometric authentication against a node or the whole network. It describes an approach for secure operation of wireless sensor networks with implemented security objectives such as confidentiality, integrity, and authentication. Then the chapter illustrates these security objectives typically employ cryptography, therefore sensor nodes should be able to compute cryptographic algorithms and provide secure tamper-resistant storage for cryptographic keys. Use of dedicated secure hardware for this purpose and security threats are discussed. Two scenarios where the biometric authentication would be appreciated are introduced – smart home and storehouse with medicaments. Biometric generation of cryptographic keys, biometric authentication in wireless network and possible attacks on biometrics are presented. When designing and verifying communication protocols using informal techniques, some security errors may remain undetected. Finally the chapter concludes by describing the formal verification methods that provide a systematic way of finding protocol flaws.

Chapter 9 describes the threats to multimedia data which are floating around in the Internet especially in the form of image data. It also shows different methods to provide security for digital images and techniques which are used to insert watermark in cover data. The chapter focuses on watermarking approaches in Hadamard transform domain. The chapter describes the approaches to make the watermarking algorithm completely automated by calculating the embedding and scaling parameters using the content of cover images. Many methods exist for calculating scaling parameter adaptively but this chapter discusses various approaches using computational intelligence to determine the optimal values of scaling and embedding parameters.

Chapter 10 aims to discuss computational aspects of lattice-based cryptographic schemes with focus on NTRU in view of the time complexity on a graphical processing unit (GPU). Polynomial multiplication algorithms, having a very important role in lattice-based cryptographic schemes, are implemented on the GPU using the compute unified device architecture (CUDA) platform in both serial and parallel ways. Compact and efficient implementation architectures of polynomial multiplication for lattice-based cryptographic schemes are presented.
Preface

There has been increased attention toward information technology and information security degrees at universities and public administration institutes around the world. The number of students studying these disciplines/degrees is also increasing; hence, this book will be very useful as an academic source for students completing these areas of study.

Security system designers and developers would benefit from reading such a book as they would gain an understanding of CI elements that are needed for developing effective and efficient security systems.

The book will also be of value to a wider range of readers who are interested in understanding CI and information security.

The Editors