

Nadia Nedjah, Ajith Abraham,
Luiza de Macedo Mourelle (Eds.)

Computational Intelligence in Information Assurance and Security

November 24, 2006

Springer

Berlin Heidelberg New York

Hong Kong London

Milan Paris Tokyo

Contents

1 Cryptography and Cryptanalysis Through Computational Intelligence

<i>E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, M.N. Vrahatis</i>	5
1.1 Introduction	6
1.1.1 Block ciphers	6
1.1.2 Public key cryptographic schemes	9
1.1.3 Elliptic Curve based cryptosystems	11
1.2 Computational Intelligence Background and Methods	12
1.2.1 Evolutionary Computation	12
1.2.2 Artificial Neural Networks	17
1.2.3 Fuzzy systems	19
1.3 Review of Cryptography and Cryptanalysis Through Computational Intelligence	20
1.4 Applying Computational Intelligence in Cryptanalysis	22
1.4.1 Cryptanalysis as Discrete Optimization Task	22
1.4.2 Cryptanalysis of Feistel Ciphers through Evolutionary Computation Methods	27
1.4.3 Utilizing Artificial Neural Networks to Address Cryptographic Problems	35
1.4.4 Artificial Neural Networks Applied on Problems Related to Elliptic Curve Cryptography	38
1.5 Ridge Polynomial Networks for Cryptography	41
1.6 Summary	46
References	47

2 Multimedia Content Protection Based on Chaotic Neural Networks

<i>Shiguo Lian</i>	55
2.1 Introduction	56
2.2 Chaotic neural networks' generation and properties	58
2.2.1 Chaotic neural network's generation	58

2.2.2 Chaotic neural network's properties suitable for data encryption	59
2.3 Multimedia content encryption based on chaotic neural networks .	63
2.3.1 Introduction to multimedia content encryption	63
2.3.2 The cipher based on chaotic neural network	64
2.3.3 Selective video encryption based on Advanced Video Coding .	68
2.4 Multimedia content authentication based on chaotic neural networks	70
2.4.1 Introduction to multimedia content authentication	70
2.4.2 The hash function based on chaotic neural network	71
2.4.3 The proposed image authentication scheme	73
2.4.4 Performance analysis	74
2.5 Future work and discussions	77
2.6 Conclusions	78
2.7 Acknowledgements	79
References	79

3 Evolutionary Regular Substitution Boxes

<i>Nadia Nedjah, Luiza de Macedo Mourelle</i>	83
3.1 Introduction	83
3.2 Preliminaries for Substitution Boxes	84
3.3 Nash Equilibrium-based Evolutionary Algorithms	86
3.4 Evolving Resilient S-Boxes	86
3.4.1 S-Box encoding and genetic operators	87
3.4.2 S-Box evaluation	88
3.5 Performance Results	91
3.6 Conclusion	92
References	92

4 Industrial Applications Using Wavelet Packets for Gross Error Detection

<i>Paolo Mercorelli, Alexander Frick</i>	93
4.1 Introduction	94
4.1.1 Modules	95
4.1.2 Gross Error Types and Examples	97
4.2 Problem Specification	99
4.2.1 Mathematical Preliminary	99
4.2.2 Noise Level Detection Problem (NLDP) and Algorithm (NLDA)	101
4.2.3 Some Remarks Regarding Wavelet Based Algorithms	101
4.3 Wavelet Based Noise Level Determination	101
4.3.1 Background and State of the Art	102
4.3.2 Noise Level Estimation: State of the Art	103
4.3.3 The Proposed New Procedure for Peak-Noise Level Detection .	104
4.3.4 Validation of Peak Noise Level Estimation	107

4.4	The Wavelet Algorithm for GEDR	110
4.4.1	Validation and Simulations	113
4.4.2	Outlier Detection Algorithm: MAD Algorithm	114
4.5	Results	115
4.5.1	Algorithm Parameterization	118
4.6	Experimental Data Sources	120
4.6.1	Dryer, Distillation and Mining Data with Outliers	122
4.6.2	Artificially Contaminated Data and Off-line, On-line Mode ..	126
4.7	Summary, Conclusions and Outlook	129
	References	130

5 Immune-inspired Algorithm for Anomaly Detection

	<i>Ki-Won Yeom</i>	133
5.1	Introduction	133
5.2	Background	135
5.2.1	The Danger Theory	135
5.2.2	Dendritic Cells as Initiator of Primary Immune Response ...	137
5.3	IDS based on Danger Theory and DCs Properties	140
5.3.1	Properties of DCs for IDS	140
5.3.2	Abstraction of Anomaly Detection Algorithm	142
5.4	DCs based Implementation of Practical Applications	145
5.4.1	A Detection of DoM Attack	146
5.4.2	Experiments and Results	149
5.4.3	A Detection of Port Scan Attack	151
5.4.4	Experiments and Results	153
5.5	Conclusion	157
	References	157

6 How to Efficiently Process Uncertainty within a Cyberinfrastructure without Sacrificing Privacy and Confidentiality

	<i>Luc Longpré, Vladik Kreinovich</i>	159
6.1	Cyberinfrastructure and Web Services	159
6.1.1	Practical Problem	159
6.1.2	Centralization of Computational Resources	160
6.1.3	Cyberinfrastructure	160
6.1.4	What Is Cyberinfrastructure: The Official NSF Definition ...	161
6.1.5	Web Services: What They Do – A Brief Summary	161
6.2	Processing Uncertainty Within a Cyberinfrastructure	162
6.2.1	Formulation of the problem	162
6.2.2	Description of uncertainty: general formulas	164
6.2.3	Error Estimation for the Results of Data Processing	166
6.2.4	How This Problem Is Solved Now	166
6.3	Need for Privacy Makes the Problem More Complex	166
6.4	Solution for Statistical Setting: Monte-Carlo Simulations	168

6.5	Solution for Interval and Fuzzy Setting	169
6.6	Summary	173
	References	174

7 Fingerprint Recognition Using a Hierarchical Approach

	<i>Chengfeng Wang, Yuan Luo, Marina L. Gavrilova and Jon Rokne</i>	179
7.1	Introduction	179
7.2	Coarse Fingerprint Matching	183
	7.2.1 Fingerprint Foreground Segmentation	184
	7.2.2 Singular Points Extraction	185
	7.2.3 Singular Points Matching	189
7.3	Topology-based Fine Matching	189
	7.3.1 Delaunay Triangulation of Minutiae Set	192
	7.3.2 Modeling Fingerprint Deformation	194
	7.3.3 Maximum Bipartite Matching	196
7.4	Experimental Results	198
7.5	Conclusions	201
	References	202

8 Smart Card Security

	<i>Kostas Markantonakis, Keith Mayes, Michael Tunstall, Damien Sauveron Fred Piper</i>	205
8.1	Introduction	205
8.2	Smart Card Specific Attacks	207
	8.2.1 Side Channel Attacks	207
	8.2.2 Fault Attacks	213
8.3	Smart Card Platform Security	218
	8.3.1 The Evolution of Smart Card Platforms	218
	8.3.2 The Different Multi-application smart card Platforms	219
	8.3.3 Java Card	221
	8.3.4 Java Card Security	223
8.4	GSM and 3G Security	225
	8.4.1 1G - TACS	226
	8.4.2 2G - GSM	226
	8.4.3 3G - UMTS	230
8.5	Summary	232
	References	233

9 Governance of Information Security: New Paradigm of Security Management

	<i>Sangkyun Kim</i>	239
9.1	Introduction	240
9.2	Rise of the Governance	241
	9.2.1 Definitions of the Governance	241
	9.2.2 Implications of the Governance	242
	9.2.3 Success Factors of the Governance	243

9.3 Why the Security Management Fails 244
 9.3.1 What the Security Management Can Do 244
 9.3.2 What the Security Management Cannot Do 246
 9.4 Governance of Corporate Security 248
 9.4.1 General Frameworks for the Governance 248
 9.4.2 Integrated Framework for the Governance of Corporate
 Security 248
 9.5 Summary 255
 References 256

List of Figures

1.1	The encryption procedure of Feistel ciphers	7
1.2	Plot of functions $g(x, y) = x^2 - y^2 \pmod{N}$ and $g(x, y) = x^2 - y^2 \pmod{N}$	23
1.3	Plot of function $h_e(x) = (x - 1)(x - 2) \pmod{N}$ and $w_e(x) = (x + 1)(x - 1)(x - 2) \pmod{N}$	24
1.4	A Pi-Sigma network (PSN) with one output unit	43
1.5	A ridge polynomial network (RPN) with one linear output unit	45
2.1	A simple neuron layer with diffusion property	60
2.2	A simple neuron layer with one-way property	60
2.3	Comparison of data block processing schemes	61
2.4	The piecewise linear chaotic map	61
2.5	The initial-value sensitivity of the chaotic Logistic map	62
2.6	The statistical results of chaotic sequence	63
2.7	Parameter generation of the chaotic neural network	65
2.8	Security test of the stream cipher.(a)Correlation between plaintext and ciphertext,(b)Correlation between different ciphertexts	68
2.9	Results of video encryption	69
2.10	Security against replacement attacks	69
2.11	The image hash based on chaotic neural network	72
2.12	The proposed image authentication scheme	74
2.13	Sensitivity of the authentication scheme. (a) original, (b) embedded, (c) tampered, (d) authentication result of 6 bit-planes, (e) authentication result of 7 bit-planes, and (f) authentication result of 8 bit-planes	76
3.1	The simplified structure of Feistel cryptographic algorithm	85
3.2	Multi-objective optimisation using Nash strategy	87
3.3	Four-point crossover of S-boxes	88
3.4	Triple-point crossover of S-boxes	89
3.5	Double-point crossover of S-boxes	90
3.6	Single-point crossover of S-boxes	90

4.1	Overview of Modules relevant to GEDR and QM	96
4.2	Example of type 1 GE. Computer-generated data with dead sensor defaulting to zero at sample number 50	98
4.3	Example of temperature measurements contaminated with outliers (top) and min, max limits	99
4.4	A set of Haar functions	102
4.5	Wavelet coefficients arranged in a tree	103
4.6	Testing Signal	108
4.7	The estimated and true variance using a threshold approach	109
4.8	The estimated and true variance using the here proposed procedure	109
4.9	A histogram for Noise Level Detection	110
4.10	The noise level for two selected measurements from the distillation data set	111
4.11	An isolated outlier	112
4.12	A multiple outlier	113
4.13	A single inverse outlier	114
4.14	A multiple (3) outlier	115
4.15	Incorrect detection of multioutliers (on sample number 227 and 228)	116
4.16	Simulation using median filter (Algower's Algorithm) with a priori knowledge on the noise	117
4.17	Simulations by using wavelet algorithm without a priori knowledge on the noise	117
4.18	Simulations by using wavelet algorithm without a priori knowledge on the noise	118
4.19	Example of a Computer-Generated Signal	119
4.20	A histogram for OADR: the MAD algorithm	120
4.21	A histogram for the OADR: the wavelet algorithm	121
4.22	A histogram for the OADR: the MAD algorithm for different data	122
4.23	A histogram for the OADR: the wavelet algorithm for different data	123
4.24	Successful outlier detection in the dryer data set	124
4.25	Outlier detection. The fine line is the original data set and the bold is the filtered one	124
4.26	Removal of noise. The fine line is the original data set and the bold is the filtered one	125
4.27	The "ged_mad_filter" applied to the Mining data. The fine line is the original data, and the bold is the filtered one	125
4.28	The "ged_wav_filter" applied to the Mining data. The fine line is the original data, and the bold is the filtered one	126
4.29	Problems when the dynamics are near the step size for the "ged_mad_filter"	127
4.30	Problems for the wavelet approach	127

4.31	The wavelet filter applied to the distillation case	128
4.32	Boiler Data Outlier Detection (1)	128
4.33	Boiler Data Outlier Detection (2)	129
4.34	Applications of both algorithms on an artificially contaminated data set	130
5.1	Dendritic-cell polarization is influenced by the type of microorganism that is recognized and the site of activation [18].	141
5.2	Indirect inflammatory signals cause DC maturation but not license DCs to drive CD4 T-cell effector functions [8].	142
5.3	The ratio of received to expected acknowledgements computed at the base station.	150
5.4	The Probability of detection of the DoM attack based on DCs .	151
5.5	Simulated false positive rate	152
5.6	Effect on different scan rates	155
5.7	Local response with random scan	156
5.8	Local response with preference scan.	157
7.1	A fingerprint and its structures.	180
7.2	Fingerprint features	181
7.3	The flowchart of our fingerprint feature extraction process	182
7.4	Orientation district template.	185
7.5	Results of segmentation algorithm on a fingerprint (300×300) .	185
7.6	Fingerprint image and block orientation field.	186
7.7	Block orientation field around different types of SPs.	187
7.8	Block orientation and template.	188
7.9	Blocks involved when computing the orientation of core	188
7.10	Four structures of Singular Points (Core marked by circle, delta marked by cross)	190
7.11	Registration of fingerprint image	191
7.12	Fingerprint fine matching flowchart	191
7.13	The Voronoi Diagram and Delaunay Triangulation of a set of points.	192
7.14	Delaunay minutiae triangle	193
7.15	Comparison of rigid transformation and non-rigid transformation in fingerprint matching	196
7.16	Strategy of matching minutiae pairs	197
7.17	Point pattern matching problem.	198
7.18	Results of SPs detection (the orientation of the core is indicated by a line) and Delaunay minutiae triangulation	199
7.19	ROC curves of general method vs. our method	200
7.20	View of a finger before and after the application of traction and torsion forces [12].	201
7.21	Performance of topology methods vs. standard methods [15,16] under distortion	201
8.1	Data Acquisition Tools.	208

8.2	Power consumption during the execution of an AES implementation.	209
8.3	Superimposed acquisitions of one clock cycle showing the data dependence of the power consumption.	210
8.4	A DPA trace.	211
8.5	The DES round function for round n	216
8.6	The typical architecture of a third generation SCOS.	219
8.7	The Java Card application development cycle and the Java Card architecture.	222
8.8	GSM authentication.	227
8.9	Compression Rounds in Comp128-1.	229
8.10	False Base Station Attack Scenario.	230
8.11	UMTS Network Authentication Vector Generation - source [2].	231
8.12	USIM Authentication Vector Handling - source [2].	231
9.1	Security governance framework.	251

List of Tables

1.1	Results for the minimization of function g (see (1.22))	26
1.2	Results for functions h_e (see (1.24)) and w_e (see (1.26)), for $N = 103 \times 107$	27
1.3	Results for DES reduced to four rounds for six different keys using $np = 20$ test pairs	31
1.4	Results for DES reduced to four rounds for six different keys using $np = 50$ test pairs	32
1.5	Results for DES reduced to six rounds for six different keys using $np = 200$ test pairs	33
1.6	Results for networks trained on the DLP and DHMP	36
1.7	Results for networks trained on the second setting of the DLP	37
1.8	Results for networks trained for the $\phi(N)$ mapping with $N = p \times q \leq 10^4$	37
1.9	Results for the second setting of the factorization problem for N ranging from 143 to 1003	38
1.10	Results for p of bit length 14, using $56 - 3 - 2$ topology	41
1.11	Results for p of bit length 20, using $80 - 3 - 2$ topology	41
1.12	Results for p of bit length 32, using $128 - 3 - 2$ topology	42
1.13	Data compression results	42
2.1	Randomness test of the produced binary sequence. The sequence is of 20000 bits with the key $K = [0.1, 0.3, 0.6, 0.8]$.	67
2.2	Test of time efficiency	70
2.3	Robustness of the proposed image hash	76
2.4	Test of computing complexity	77
3.1	Characteristics of the best S-boxes \mathcal{S}^+ by Millan et al. [11], Clark et al. [12] and our approach	91
5.1	Weights for the signal processing function	145
5.2	Parameters for secure e-mail	149
5.3	Parameters for detecting port scanning	153
5.4	Network simulator environments	155
7.1	Coarse Matching Rules	189

7.2	Performance comparison between [11] and the proposed algorithms on database1	198
7.3	Computation complexity of our <i>Fine Matching Stage</i>	199
9.1	What the security management can do	245
9.2	General frameworks for the governance	249
9.3	Limitations of general frameworks	250
9.4	Key factors of the governance framework for corporate security .	250