## Contents

**Part I  Bio-inspiring Systems in Cyber Security**

1. A Bio-inspired Comprehensive Distributed Correlation Approach for Intrusion Detection Alerts and Events  
   Ayman M. Bahaa-Eldin  
   1.1 Introduction  
   1.1.1 IDS Correlation Problem Definition  
   1.1.2 Article Organization  
   1.2 Related Work  
   1.2.1 Distributed and Bio Inspired Intrusion Detection  
   1.2.2 Distributed Correlation  
   1.2.3 Agents in IDS and Correlation  
   1.2.4 Comprehensive Approach Model for IDS Alert Correlation  
   1.2.5 Distributed Agent Correlation Model  
   1.2.6 IDSs Correlation Agents  
   1.2.7 INFOSEC Tools Agents  
   1.2.8 System and Application Log Agents  
   1.2.9 DACM Central Agent  
   1.2.10 Response Agent  
   1.2.11 Learning Agent  
   1.2.12 The Knowledge Base and Security Policy  
   1.2.13 DACM Components  
   1.2.14 Implementation Scope and Performance Enhancement  
   1.3 DACM Design and Algorithms  
   1.3.1 IDS Alert Correlation  
   1.3.2 Modified CAM Time  
   1.3.3 DACM Individual Agents  
   1.3.4 Implementation Environment  
   1.4 DACM Results and Analysis  
   1.4.1 CRIAS Data Set  
   1.4.2 IDS Alerts Correlation Results  
   1.4.3 DACM Components Results
4 Bio-inspiring Techniques in Watermarking Medical Images: A Review

Mona M. Soliman, Aboul Ella Hassanien and Hoda M. Onsi

4.1 Introduction

4.2 Bio-inspiring Computing

4.2.1 Artificial Neural Networks

4.2.2 Evolutionary Algorithms

4.2.3 Genetics Algorithms

4.2.4 Swarm Intelligence

4.3 Medical Image Watermarking: Classification and Generic Model

4.3.1 Medical Watermarking Classification

4.3.2 Generic Medical Image Watermarking System

4.4 BI in Medical Image Watermarking

4.4.1 Artificial Neural Networks in Medical Image Watermarking

4.4.2 Genetic Algorithms in Medical Image Watermarking

4.4.3 Swarms Intelligent in Medical Image Watermarking

4.4.4 Hybrid Bio-inspiring Systems in Medical Watermarking

4.5 Watermarking Assessment Measures

4.5.1 Imperceptibility or Transparency

4.5.2 Robustness

4.6 Conclusions and Future Directions

References

5 Efficient Image Authentication and Tamper Localization Algorithm Using Active Watermarking

Sajjad Dadkhah, Azizah Abd Manaf and Somayeh Sadeghi

5.1 Introduction

5.2 Related Work

5.2.1 Digital Image Authentication Methods

5.3 The Proposed Algorithm

5.3.1 The Proposed Watermarking Scheme

5.3.2 The Proposed Tamper Detection Scheme

5.4 Experimental Results

5.4.1 Watermark Quality Experiments Result

5.4.2 Tamper Detection Experiments Results

5.4.3 Deletion and Copy-Move Tampering Attacks

5.4.4 Bit Tampering Experiments Results

5.5 Conclusion

References
Part II Mobile Ad Hoc Networks and Key Managements

6 TARA: Trusted Ant Colony Multi Agent Based Routing Algorithm for Mobile Ad-Hoc Networks ................................................. 151
Ayman M. Bahaa-Eldin
6.1 Introduction .................................................. 151
6.2 Background .................................................. 153
   6.2.1 Mobile Ad-Hoc Networks .............................. 153
   6.2.2 Swarm Intelligence ..................................... 161
6.3 Trusted Routing Protocols for MANETs ................... 163
   6.3.1 Examples of Trusted Routing Protocols ................. 163
6.4 Trusted Ant Colony Based Routing Algorithm for Mobile Ad-Hoc Networks .................................................. 169
   6.4.1 Routing Table Data Structure ....................... 171
   6.4.2 Node Trust Evaluation ................................. 171
   6.4.3 Route Discovery ........................................ 172
   6.4.4 Route Selection and Route Failure Handling .......... 175
   6.4.5 Route Maintenance .................................... 175
   6.4.6 TARA Complexity Analysis ........................... 176
6.5 Performance Evaluation of TARA .......................... 177
   6.5.1 Simulation Environment ............................... 177
   6.5.2 Simulation Results and Analysis ..................... 178
6.6 Conclusion .................................................. 181
References ....................................................... 182

7 An Overview of Self-Protection and Self-Healing in Wireless Sensor Networks .................................................. 185
Tarek Gaber and Aboul Ella Hassanien
7.1 Introduction .................................................. 185
7.2 Wireless Sensor Networks Architecture ................... 186
7.3 Autonomic Computing ....................................... 187
   7.3.1 Autonomic Computing Characteristic ................. 188
   7.3.2 Autonomic Computing Elements ....................... 189
7.4 Self-Protection .............................................. 190
   7.4.1 Self-Protection in WSN ............................... 191
7.5 Self-Healing ................................................ 193
7.6 Self-Healing in WSNs ...................................... 195
   7.6.1 Existing Solution of WSN with Self-Healing .......... 195
7.7 BiSNET: Biologically-Inspired Architecture for Sensor NETworks .................................................. 198
   7.7.1 Overview of BiSNET ................................. 198
   7.7.2 Self-Healing in BiSNET ............................ 199
7.8 Conclusions .................................................. 200
References ....................................................... 201
8 Cybercrime Investigation Challenges: Middle East and North Africa
Mohamed Sarrab, Nasser Alalwan, Ahmed Alzahrani and Mahdi Kordestani
8.1 Introduction 204
8.2 Related Work 205
8.3 Conceptualizing Cybercrime 205
8.4 State of Information Security in North Africa and Middle East 206
8.4.1 Information Technology Infrastructure 207
8.4.2 Growth of IT User 207
8.4.3 Lack of Regulations and Training of Law Enforcements 208
8.5 Internet Users and Population Statistics for Middle East 208
8.6 Internet Users and Population Statistics for North Africa 210
8.7 Case Study 213
8.7.1 Stuxnet 213
8.7.2 W32.Disttrack 214
8.7.3 Duqu 216
8.7.4 Flame 218
8.8 Discussion 219
8.9 Challenges 220
8.10 Conclusion 221
References 222

9 Multilayer Machine Learning-Based Intrusion Detection System
Amira Sayed A. Aziz and Aboul Ella Hassanien
9.1 Introduction 226
9.2 Background 227
9.2.1 Intrusion Detection Systems 227
9.2.2 Genetic Algorithm 228
9.2.3 Principal Component Analysis 228
9.2.4 Artificial Immune System 230
9.2.5 Negative Selection Algorithm 230
9.3 The Proposed Multilayer Machine Learning-Based IDS 231
9.3.1 Layer I: Feature Selection Based Principal Components Analysis Layer 232
9.3.2 Layer II: Anomaly Detection-Based Genetic Algorithm with Negative Selection Layer 233
9.3.3 Layer III: Detected Anomalies Classification Layer 234
10 An Improved Key Management Scheme with High Security in Wireless Sensor Networks .......................... 249
D. Satish kumar, N. Nagarajan and Ahmad Taher Azar
10.1 Introduction .................................................. 250
10.2 Related Work .................................................. 251
10.3 INTK Scheme .................................................. 253
   10.3.1 Initial INTK Setup Process .......................... 255
   10.3.2 INTK Structure Operation Algorithm ............... 257
   10.3.3 INTK Security Feature ............................... 258
10.4 Simulation Environment ..................................... 259
10.5 Results and Discussion ..................................... 260
10.6 Conclusion ................................................... 263
References ......................................................... 263

11 Key Pre-distribution Techniques for WSN Security Services .......... 265
Mohamed Mostafa M. Fouad and Aboul Ella Hassanien
11.1 Introduction .................................................. 265
11.2 Security Services for the WSNs ............................. 266
   11.2.1 Authentication ........................................ 266
   11.2.2 Data Confidentiality .................................. 267
   11.2.3 Data Integrity ......................................... 267
   11.2.4 Availability .......................................... 268
   11.2.5 Data Freshness ....................................... 268
   11.2.6 Self-Organization ..................................... 268
   11.2.7 Time Synchronization .................................. 269
   11.2.8 Secure Localization ................................... 269
11.3 WSN's Threat Model ......................................... 269
11.4 Security Attacks on Sensor Networks .......................... 270
11.5 Key Distribution Techniques for Distributed WSNs ................. 272
11.6 Pairwise Key Distributed Schemes ............................ 273
   11.6.1 Polynomial Based Key Pre-distribution Scheme ....... 274
   11.6.2 Probabilistic Key Pre-distribution (PRE) ............. 275
   11.6.3 Q-Composite Random Key Pre-distribution Scheme .... 276
   11.6.4 Random Pairwise Keys Scheme ........................ 276

9.4 Experimental Results and Discussion ............................ 235
   9.4.1 Data Set ............................................... 235
   9.4.2 Results ............................................... 236
9.5 Conclusion and Future Work .................................... 245
References ......................................................... 246
11.6.5 Polynomial Pool-Based Key Pre-distribution Scheme ........................................ 276
11.6.6 Location Based Pairwise Key Scheme ................................................................. 278
11.6.7 Time Based Pairwise Key Scheme ..................................................................... 279
11.7 Conclusion and Future Works .............................................................................. 280
References ................................................................................................................. 281

Part III Biometrics Technology and Applications

12 Fusion of Multiple Biometric Traits: Fingerprint, Palmprint and Iris .................... 287
N. L Manasa, A Govardhan and Ch Satyanarayana

12.1 Introduction .............................................................................................................. 288
  12.1.1 Kinds of Information Fusion ........................................................................... 293

12.2 Motivation and Challenges .................................................................................... 294
  12.2.1 Fusion of Multiple Representations of Single Biometric Trait ....................... 294
  12.2.2 Fusion of Multiple Biometric Traits ............................................................... 295

12.3 Contributions ......................................................................................................... 297

12.4 Fusion of Multiple Representations of Individual Fingerprint, Palmprint and Iris 298
  12.4.1 Global Feature Extraction ............................................................................... 299
  12.4.2 Local Feature Extraction ................................................................................. 301
  12.4.3 Feature Fusion .................................................................................................. 302
  12.4.4 Feature Matching .............................................................................................. 304

12.5 Fusion of Multiple Biometric Traits: Fingerprint, Palmprint, Iris ....................... 304
  12.5.1 Parallel Architecture Based Fusion ................................................................. 309
  12.5.2 Hierarchical-Cascading Architecture Based Fusion ....................................... 311

12.6 Description of Databases ....................................................................................... 315

12.7 Discussion and Future-Work .................................................................................. 316

References ..................................................................................................................... 318

13 Biometric Recognition Systems Using Multispectral Imaging .............................. 321
Abdallah Meraoumia, Salim Chitroub and Ahmed Bouridane

13.1 Introduction .............................................................................................................. 322
13.2 Related Works ......................................................................................................... 323

13.3 Multimodal Biometric System ............................................................................... 324
  13.3.1 Fusion at Image Level ...................................................................................... 324
  13.3.2 Fusion at Matching Score Level ...................................................................... 325
13.4 Multispectral Palmprint Identification .......................... 325
13.4.1 Multispectral Palmprint Image .............................. 325
13.4.2 Multispectral Palmprint Database ......................... 326
13.4.3 Palmprint Preprocessing .................................. 326
13.4.4 Unimodal Identification System Test Results .............. 327
13.4.5 Multimodal Identification System Test Results .......... 339
13.5 Reliability of Multispectral Imaging ........................... 342
13.6 Summary and Conclusions ..................................... 344
References ............................................................ 345

14 Electrocardiogram (ECG): A New Burgeoning Utility for Biometric Recognition ............................................. 349
Manal Tantawi, Kenneth Revett, Abdel-Badeeh Salem and M. Fahmy Tolba
14.1 Introduction ...................................................... 350
14.2 Heart Fundamentals ............................................ 352
14.2.1 Heart Anatomy ............................................ 352
14.2.2 Flow of Blood ............................................. 352
14.2.3 The Electrical Activity of the Heart ....................... 352
14.3 Electrocardiogram .............................................. 353
14.3.1 ECG and Biometrics ........................................ 354
14.3.2 ECG Motivation ............................................ 354
14.3.3 ECG Challenges ............................................ 354
14.4 Existing ECG Based Biometric Systems ......................... 355
14.4.1 Fiducial Based Systems .................................... 356
14.4.2 Non-Fiducial Based Systems ............................... 361
14.4.3 Combined Fiducial and Non-fiducial Based Systems ......... 367
14.4.4 Fiducial Versus Non-fiducial Based Systems ............... 369
14.5 Methodology ..................................................... 371
14.5.1 Data Preparation ........................................... 371
14.5.2 Preprocessing .............................................. 371
14.5.3 Feature Extraction ......................................... 372
14.5.4 Feature Reduction ......................................... 372
14.5.5 Classification ............................................... 374
14.6 Results and Discussion ....................................... 375
14.6.1 The Global Phase (Significance of the Structure Parts) .... 376
14.6.2 Local Phase (Significance of Coefficients) ................. 378
14.6.3 Generalization .............................................. 379
14.7 Conclusion and Future Work .................................. 379
References ............................................................ 380
15 Image Pre-processing Techniques for Enhancing the Performance of Real-Time Face Recognition System

Using PCA

Behzad Nazarbakhsh and Azizah Abd Manaf

15.1 Introduction

15.2 Literature Survey

15.2.1 Image Acquisition

15.2.2 Segmentation

15.2.3 Localization

15.2.4 Normalization

15.2.5 Feature Selection and Extraction

15.2.6 Classification

15.3 Methodology

15.3.1 Image Preprocessing Using for Detection

15.3.2 Color Conversion and Segmentation

15.3.3 Localization

15.3.4 Normalization

15.3.5 Face Recognition

15.3.6 Feature Extraction

15.3.7 Classification

15.4 Proposed Method

15.4.1 Color Conversion

15.4.2 Segmentation

15.4.3 Eyes and Mouth Identification and Localization

15.4.4 Average Half Face

15.4.5 Feature Extraction and Classification

15.5 Experimental Result

15.5.1 Understanding the Ratio of Training to Test Images Numbers Needed

15.5.2 Changing the Training and Test Image Combination

15.5.3 Calculating False Positive Rate and Sensibility

15.5.4 Performance Comparison of Proposed Method with the Similar Recognition Framework

15.6 Conclusion

References

16 Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues

Reham Amin, Tarek Gaber, Ghada ElTaweel and Aboul Ella Hassanien

16.1 Introduction

16.2 Traditional Authentication Methods

16.2.1 Knowledge-Based Authentication

16.2.2 Object-Based Authentication
18 Data and Application Security in Cloud
Rajesh P. Barnwal, Nirnay Ghosh and Soumya K. Ghosh
18.1 Introduction
18.2 Cloud Computing
18.2.1 Security in Cloud Computing
18.3 Data and Application Security
18.3.1 Secure Data Transmission
18.3.2 Secure Data Storage and Integrity Verification
18.3.3 Prevention Against Attacks
18.3.4 Isolation of Customer-Specific Data and Application
18.4 Research Directions
18.5 Conclusion
References

19 Security Issues on Cloud Data Services
Nour Zawawi, Mohamed Hamdy El-Eliemy, Rania El-Gohary and Mohamed F. Tolba
19.1 Introduction
19.2 Security Issues
19.2.1 Traditional Security Challenges
19.3 Data Integrity
19.4 Data Availability
19.5 Data Confidentiality
19.6 Security and Trust Cloud Data Service
19.6.1 EWRDN Service Model
19.6.2 EWRDN Utilization of Resources
19.7 Conclusion
References

20 A Reputation Trust Management System for Ad-Hoc Mobile Clouds
Ahmed Hammam and Samah Senbel
20.1 Introduction
20.2 Related Work
20.3 PlanetCloud in Brief
20.3.1 Client Agent
20.3.2 Cloud Agent
20.3.3 Resource Server
20.4 Proposed Trust management System for Ad-Hoc Mobile Cloud TMC
20.4.1 TMC System Design
20.4.2 Simulator
20.4.3 Comparison Between TMC and Existing Trust Management Systems for MANET