2011 Seventh International Conference on Computational Intelligence and Security

(CIS 2011)

Sanya, Hainan, China
3 – 4 December 2011

Pages 788-1588
Analysis of the Authentication Protocols Based on Game Theory - An Improvement of L.H. Nguyen Scheme ................................................................. 788
   Xinghua Li, Lingjuan Deng, Yuan Zhang, Dan Yang, and Jianfeng Ma

Design of a Digital Forensics Evidence Reconstruction System for Complex and Obscure Fragmented File Carving ...................................................... 793
   Vrizlynn L.L. Thing, Tong-Wei Chua, and Ming-Lee Cheong

Evaluating the Effect of Loading Forensic Tools on the Volatile Memory for Digital Evidences ......................................................................................... 798
   Zhen Su and Lian Hai Wang
Hierarchical ID-Based Blind Signature from Lattices ..............................................................803
Chen Liang, Cui Yongquan, Tang Xueming, Hu Dongping, and Wan Xin

Identity-based SIP Authentication and Key Agreement .........................................................808
Wu Shao Bo and Li Cheng Shu

Obtaining the Resonant Frequency of the Bubble in the Ship Wake by ANSYS ..........................812
Zhang Qun and Yingmin Wang

Security Authentication Scheme Based on Certificateless Signature and Fingerprint Recognition .................................................................817
Zhu Yanqiong, Xu Hui, and Gao Zhan

Security Problems and Countermeasures with Commercial Banking Computer Networks .................................................................821
Yun Cheng Liu, Xingchun Sun, and Xiaoqin Mao

Synthesis Algorithm of Homologous Detection Based on Analytic Hierarchy Process ..........826
Baojing Cui, Ce Bian, Tao Guo, Yongle Hao, and Jianxin Wang

Systematical Vulnerability Detection in Browser Validation Mechanism ..............................831
Zeng Chufeng and Wang Qingxian

The Analysis of Influence Factors of the Confidence Level on University Students’ Network Shopping .................................................................837
Junfeng He and Hui Sun

Traitor Tracing and Revocation Mechanisms with Privacy-Preserving .................................842
Yi Ding and Lei Fan

Cryptography and Cryptanalysis

2-out-of-2 Rational Secret Sharing in Extensive Form ..............................................................847
Yilei Wang and Qiuliang Xu

A Construction of Balanced Odd-variable Boolean Function with Optimum Algebraic Immunity .................................................................852
Yin Dong Chen

A New Cross-realm Group Password-based Authenticated Key Exchange Protocol .............856
Qing Dai, Xiufeng Zhao, Qiuliang Xu, and Han Jiang

A Novel Group Signature Scheme Based on NTRU ..............................................................861
Junping Yao, Zefeng Dong, and Xinshe Li

A Protocol of Privacy-Preserving Closest Pair in Two Dimensional Space ..........................865
Yong-long Luo, Chao Cheng, Cai-xia Chen, and Hong Zhong

A Watermarking-based Visual Cryptography Scheme with Meaningful Shares ..................870
Han Yan-yan, Cheng Xiao-ni, and He Wen-cai

Accelerating Block Cryptography Algorithms in Procedure Level Speculation ..................874
Yaobin Wang, Hong An, Zhiqin Liu, Kang Xu, and Wanli Dong

An ID-based (k, t, n) Threshold Group Signature Scheme ....................................................878
Wei Fu and Guang-liang Liu
An Image Encryption Algorithm Based on Scrambling and Substitution Using Hybrid Chaotic Systems .................................882
    Xiang Fei and Guo Xiao-cong

An Improved Signcryption with Proxy Re-encryption and its Application .........................................................886
    Caiwen Wang and Xiaojun Cao

An Improvement and a New Design of Algorithms for Seeking the Inverse of an NTRU Polynomial ........................................891
    Na Zhao and Shenghui Su

Attack on the Cryptosystem Based on DLP .................................896
    Xiaobo Feng and Mingqiang Wang

Attribute-Based Authenticated Key Exchange Protocol with General Relations ............................................900
    Hao Wang, Qiuliang Xu, Han Jiang, and Rui Li

Attribute-based Signcryption with Ciphertext-policy and Claim-predicate Mechanism .........................................905
    Changji Wang and Jiasen Huang

Certificateless Broadcast Signcryption with Forward Secrecy ..................................................................................910
    Ming Luo, Chun-hua Zou, and Jianfeng Xu

Co-Z Addition Operation of Hessian Curve ........................................................................................................915
    Leibo Li and Tao Zhan

Concurrent Non-malleable Statistically Hiding Commitment ...........................................................................920
    Rui Li, Qiuliang Xu, and Hao Wang

Cryptoanalysis and Improvement of Verifier-based Key Agreement Protocol in Cross-Realm Setting ......................925
    Jing-feng Li, Wei-feng Guo, Lai-shun Zhang, and Yun-peng Li

Differential Energy Watermarking Based on Macro-block Prediction ..................................................................930
    Qian Zeng and Guorui Feng

Efficient Password-Based Authenticated Key Exchange from Lattices ..............................................................934
    Yi Ding and Lei Fan

Elliptic Curve Isogenies to Resist Differential Side-Channel Analysis Attacks ................................................939
    Keke Wu, Huiyun Li, XuCheng Yin, and Guoqing Xu

Hierarchical Identity-based Broadcast Encryption Scheme on Lattices ..............................................................944
    Zhang Jinman and Chen Qin

K-times Proxy Re-encryption .....................................................................................................................949
    Xu An Wang, Ziqing Wang, Yi Ding, and Shujun Bai

Multi-Undeniable Signature Schemes ..............................................................................................................954
    Shen Xunxun, Xu Maozhi, and Zhao Yanhui

Novel Quantization Watermarking Based on Random Angle Modulation .......................................................959
    Xinzhan Zhu and Shuoling Peng

Optimized Approach for Computing Multi-base Chains .....................................................................................964
    Xinchun Yin, Ting Yang, and Jianting Ning
Proxy Re-encryption with Keyword Search from Anonymous Conditional Proxy

Wei Dong Zhong, Xu An Wang, Ziqing Wang, and Yi Ding

VVCS: Verifiable Visual Cryptography Scheme

Han Yanyan, Cheng Xiaoni, Yao Dong, and He Wencai

Access Control and Protection

A Generic Scheme for the Construction of Contextual Signatures with Hash Function in Intrusion Detection

Yuxin Meng and Lam-for Kwok

A New Approach for Adaptive Intrusion Detection

Hassina Bensefia and Nacira Ghoulami

A Security API for Multimodal Multi-biometric Continuous Authentication

Adriana Esmeraldo de Oliveira and Gustavo Henrique Matos Bezerra Motta

A Wavelet-Based Detection Approach to Traffic Anomalies

Dingde Jiang, Peng Zhang, Zhengcheng Xu, Cheng Yao, and Wenda Qin

An Access Control Mode Based on Information Flow Graph

Wang Chao, Chen Xing Yuan, and Li Na

An Enhanced Role-Based Access Control Mechanism for Hospital Information Systems

Chen-Guang He, Cun-Zhang Cao, and Shu-Di Bao

Fast Network Traffic Anomaly Detection Based on Iteration

Hua Jiang and Liaojun Pang

Kernel-based Behavior Analysis for Android Malware Detection

Takamasa Isohara, Keisuke Takemori, and Ayumu Kubota


Jozsef Hegedus, Yoan Miche, Alexander Ilin, and Amaury Lendasse

Performance Analysis of the Single Pattern Matching Algorithm Based on Prefix Searching

Wu Xi-hong

Property-Based Remote Attestation Oriented to Cloud Computing

Si Yuan Xin, Yong Zhao, and Yu Li

Research and Implementation of DPA-resistant SMS4 Block Cipher

Xiaoyi Duan, Ronglei Hu, and Xiu Ying Li

Research of Access Control in Electronic Medical Record Based on UCON

Ju Jian Guo, Chen Weihe, and Zhan Yong Zhao

Research on Access Control Mechanism for Digital Products Trading

Li Fenghua, Yu Yinyan, Li Dongdong, and Zhang Jinhui
Study on Role-Based Access Control with Time Constraint
Zhenghong Liu, Yuhong Jia, and Tieli Sun

Using a Dynamic K-means Algorithm to Detect Anomaly Activities
Li Han

Pattern Recognition and Knowledge Discovery

A New Algorithm for Auto-Exposure Based on the Analogy Histogram
Zhang Haifeng, Cao Jianzhong, Tang Linao, and Wang Huawei

A Novel Subspace Discriminant Locality Preserving Projections for Face Recognition
Wei He, Wen-Sheng Chen, and Bin Fang

A Saliency Detection Model Based on Multi-feature Fusion
Zheng Yang, Liu Chunping, Wang Zhaohui, Ji Yi, and Gong Shengrong

A Secondary Image Denoising Model Based on the Local Energy Operator
Xu Chen, Sun Xiao-li, and Li Min

Active Contours with Adaptively Normal Biased Gradient Vector Flow External Force
Hengbo Zhao and Li Xiong Liu

Adaptive Filter for Color Impulsive Removal Based on the HSI Color Space
Shi Yan-xin and Cheng Yong-mei

An Efficient Linear Text Segmentation Algorithm Using Hierarchical Agglomerative Clustering
Ji-Wei Wu, Judy C.R. Tseng, and Wen-Nung Tsai

Automatic Detection of Lumina in Mouse Liver Immunohistochemical Color Image
Using Support Vector Machine and Cellular Neural Network
Wang Hui, Zhou Zhi Guo, and Jie Long Mei

Automatic Parameter Determination Based on a Modified Discriminant Criterion for Face Recognition
Taiquan Huang and Wen-Sheng Chen

Cell Nuclei Detection in Histopathological Images by Using Multi-curvature Edge Cue
Baochuan Pang, Long Zhou, Wu Zeng, and Xinge You

Construction of a Bilingual Cognitive Property Knowledgebase
Bin Li, Haibo Kuan, Xiaohe Chen, Xuri Tang, and Chen Chen

Contours-Matching in Building Reconstruction from a Single Image
Xin Zheng, Xiumin Zhang, Fuqing Duan, and Wei Liu

Efficient e-Discovery Process Utilizing Combination Method of Machine Learning Algorithms
Tae Rim Lee, Bon Min Goo, Hun Kim, and Sang Uk Shin

Face Recognition with Statistical Local Line Binary Pattern
Zheng-Chun Sun and Jian Cheng

Face Reconstruction from Skull Based on Partial Least Squares Regression
Donghua Huang, Fuqing Duan, Qingqiong Deng, Zhongke Wu, and Mingquan Zhou
Schistosoma Cercariae Image Recognition via Sparse Representation .......................................................... 1206
    Shenhai Yan, Yang Liu, and Xiantong Huang

Soft-Voting Classification Using Locally Linear Reconstruction ................................................................. 1211
    Xiaohui Tian and Rong Wang

Sparse Representation for Multi-Label Image Annotation ............................................................................ 1215
    Bingxin Xu and Ping Guo

Speech Feature Analysis Using Temporal Linear Embedding ......................................................................... 1220
    Lifang Xue and Xiushuang Yi

Streamline-based Visualization of 3D Explosion Fields .................................................................................. 1224
    Yi Wang, Wenyao Zhang, and JianGuo Ning

The Application of Binary Particle Swarm Algorithm in Face Recognition .................................................. 1229
    Guojian Cheng, Caizun Shi, Kai Zhu, and Kevin Gong

The Iterative Regularization Method Based on Image Decomposition Model .............................................. 1234
    Li Min, Xu Chen, Sun Xiaoli, and Zhang Weiqiang

The Multispectral Image Edge Detection Based on Clifford Gradient ......................................................... 1238
    Hui Liu, Chen Xu, and Wenming Cao

Using the Callback Function Realization Touch Screen Gestures Recognition of Computer ...................... 1243
    Ma Shuang Chong

Data Mining

A Boundary Detection Algorithm of Clusters Based on Dual Threshold Segmentation .................................. 1246
    Baozhi Qiu and Shuang Wang

A Combined Music Label Propagation Model ................................................................................................. 1251
    Jing Cai, Heng Li, and Bo Lang

A Method for New Word Extraction on Chinese Large-scale Query Logs .................................................... 1256
    Rui Sun, Peng Jin, and Juan Lai

A New Community Structure Detection Method Based on Structural Similarity ........................................ 1260
    Qi Luo

A Real Time Multi-Scale Correlation Analysis Method and its Application on the Data Mining in Thermodynamic Process ................................................................. 1263
    Wang Qi and Liu Xin-Ping

A Simple But Effective Stream Maximal Frequent Itemset Mining Algorithm .............................................. 1268
    Haifeng Li and Ning Zhang

A Weighted K-hyperline Clustering Algorithm for Mixing Matrix Estimation on Bernoulli-Gaussian Sources ............................................................................................................... 1273
    Jun-jie Yang and Hai-lin Liu

An Empirical Study on Credit Scoring Model for Credit Card by Using Data Mining Technology ................ 1279
    Wei Li and Jibiao Liao
An Improved ID3 Based on Weighted Modified Information Gain

Chun Guan and Xiaoqin Zeng

Analysis on Cloud Computing-based Logistics Information Network Mode

Xing Wang

Another View of the Features in Supervised Chinese Word Sense Disambiguation

Peng Yuan Liu

Application of Cloud Storage in Traffic Video Detection

Ru Xue, Zong-Sheng Wu, and A-Ning Bai

Approximation Kernel 2DPCA by Mixture of Vector and Matrix Representation

Lin Wang and Xiuling Zhou

Clustering Based Image Denoising Using SURE-LET

Wu Zeng, Long Zhou, Xiubao Jiang, Xinge You, and Mingming Gong

Data Mining Technique in the Internal Auditing of Enterprise Groups

Aijun Yang and Ping Song

Data Sources of Webometrics

Shi Longqing and Zhao Qingfeng

Measuring Semantic Relatedness between Words Using Lexical Context

Wei He, Xiaoping Yang, and Dupei Huang

Methodology for Statistical Distribution Determination of Various Data Sources

Changqing Liu and Wencai Luo

Neural Network in the Application of EEG Signal Classification Method

Huaping Jia

Normalizing Modularity Matrices for Data Clustering

Rong Wang

Pattern Recognition with Spatial Data Mining in Web: An Infrastructure to Engineering of the Urban Cadaster

André Fabiano de Moraes and Lia Caetano Bastos

Promotion Analysis Based on Fitting in Multi-Level Space

Li Sun, Ming Zhu, and Jiyun Li

Research on Characteristics of Plates on Chinese Stock Market

Peng Lin and Jianhui Yang

Research on Industrial Building’s Reliability Assessment Based on Projection Pursuit Model

Zhang Lei and Jie Liu

Research on Privacy-preserving in Distributed Mining Based on the Attribute Similarity

Qiu Lu and Xiao-hui Cheng

Sequential Bayesian Method for Formulating Uncertainty in Sparse Data

Changqing Liu and Wencai Luo
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Similarity Matching over Uncertain Time Series</td>
<td>1357</td>
</tr>
<tr>
<td>Yanfei Zuo, Guohua Liu, Xiaoli Yue, Wei Wang, and Honghua Wu</td>
<td></td>
</tr>
<tr>
<td>Simplified Business Process Model Mining Based on Structuredness Metric</td>
<td>1362</td>
</tr>
<tr>
<td>Weidong Zhao, Xi Liu, and Anhua Wang</td>
<td></td>
</tr>
<tr>
<td>Spectral Clustering and its Research Progress</td>
<td>1367</td>
</tr>
<tr>
<td>Fu Chuanyi, Chen Huan-dong, and Xing Jieqing</td>
<td></td>
</tr>
<tr>
<td>SVM Combined with FCM and PSO for Fuzzy Clustering</td>
<td>1370</td>
</tr>
<tr>
<td>Yifang Yang, Guoqiang Chen, and Yanchun Guo</td>
<td></td>
</tr>
<tr>
<td>The Classification of k-anonymity Data</td>
<td>1374</td>
</tr>
<tr>
<td>Lin Bing-chun and Liu Guohua</td>
<td></td>
</tr>
<tr>
<td>The Estimation of Mixing Matrix Based on Bernoulli-Gaussian Model</td>
<td>1379</td>
</tr>
<tr>
<td>Jiechang Wen and Taowen Wang</td>
<td></td>
</tr>
<tr>
<td>The Finite Element Analysis of the Electromagnetic Levitation System Based on the Large Air Gap</td>
<td>1384</td>
</tr>
<tr>
<td>Zhengfeng Ming and Rui Wen</td>
<td></td>
</tr>
<tr>
<td>The Problem about Grey Incidence Cluster Analysis</td>
<td>1387</td>
</tr>
<tr>
<td>Yanping Cao and Chunmei Gong</td>
<td></td>
</tr>
<tr>
<td>TKNN: An Improved KNN Algorithm Based on Tree Structure</td>
<td>1390</td>
</tr>
<tr>
<td>Li Juan</td>
<td></td>
</tr>
<tr>
<td><strong>System Analysis and Modeling</strong></td>
<td></td>
</tr>
<tr>
<td>A Data Distribution Platform Based on Event-Driven Mechanism</td>
<td>1395</td>
</tr>
<tr>
<td>Wang Wei, Tan Enmin, and Feng Bing</td>
<td></td>
</tr>
<tr>
<td>A General Edge Detection Method Based on the Shear Transform</td>
<td>1400</td>
</tr>
<tr>
<td>Qiguang Miao, Pengfei Xu, Weisheng Li, and Hai Zhu</td>
<td></td>
</tr>
<tr>
<td>A Lower Bound for the Smarandache Function Value</td>
<td>1405</td>
</tr>
<tr>
<td>Guo Yanchun, Ren Ganglian, and Yang Yifang</td>
<td></td>
</tr>
<tr>
<td>A New Method for Interval Multiple Attribute Decision Making Based on Minimum Variance and Approach Degree</td>
<td>1408</td>
</tr>
<tr>
<td>Zhenhai Ai</td>
<td></td>
</tr>
<tr>
<td>A Novel Two-stage Analysis Method for Customer’s Requirement</td>
<td>1413</td>
</tr>
<tr>
<td>Hai Zhu, Zengfa Dou, and Wengang Zhou</td>
<td></td>
</tr>
<tr>
<td>A Safety Framework and Alarming Model for Train Operation Environment Based on CPS</td>
<td>1418</td>
</tr>
<tr>
<td>Xinhong Hei, Lining Chang, Weigang Ma, and Guo Xie</td>
<td></td>
</tr>
<tr>
<td>Achievement of Proxy Cache System for Streaming Media Based on Patch Algorithm</td>
<td>1422</td>
</tr>
<tr>
<td>Weitao Ha</td>
<td></td>
</tr>
<tr>
<td>An Implementation Method for Converting the Erhu Music from Wav to Mid</td>
<td>1425</td>
</tr>
<tr>
<td>Ziqing Nie and Shiyong Yang</td>
<td></td>
</tr>
</tbody>
</table>
Analysis of the Impact of Polarization Mode Dispersion on Optical Fiber
Wei Zhao .................................................. 1430

Analytical Models for Data Dependence Violation Checking in TLS
Xin Lai, Cong Liu, Zhiying Wang, and Quanyou Feng .............. 1433

CFD Numerical Simulation of Exhaust Muffler
Jun Chen and Xiong Shi .................................. 1438

Closed-loop Supply Chain Network Horizontal Integration Problem
Yang Yuxiang and Zhou Gen-gui .............................. 1442

Computer Realization of Quadratic Spline Interpolation
Feng Tianxiang and Liu Hongxia ............................. 1447

Constructing the Expandability Web Service Based Linux
Rong Shan .................................................... 1451

Co-op Advertising Analysis within a Supply Chain Based on the Product Life Cycle
Hong Zhang and Sheng Zhong ............................... 1456

Correlation Factor Analysis of FEA Model Simplification Methods of Printed Circuit Board
Zou Su, Li Chuanri, Xu Fei, and Qiao Liang ................. 1461

DBS Application to Chinese Adjectives
Qixiang Feng, Degen Huang, Xiuying Li, and Rongpe Wang ........ 1466

Design and Implement of SerialPort Class on Upper Machine System
Fu Chuanyi, Zhan Jinmei, and Chen Juntao .................. 1471

Design and Implementation of Bus Net Routing Algorithm
Min Luo, Haiquan Wang, Chunhe Xia, Lihua Wang, and Ya Wang .... 1474

Design of Instrument Control System Based on LabView
Kang Jianhua, She Fangyi, Yang Fangzheng, and Wang Tao ....... 1479

Dynamic Risk Measurement of Futures Based on Wavelet Theory
Jianhui Yang and Peng Lin ................................... 1484

Existence of Almost Periodic and Almost Automorphic Solutions for Second Order Differential Equations
Lan Li ......................................................... 1488

Experimental Study the Measurement of Acoustic Wave Flight Time under Strong Noise in the Boiler
Feng Tian and Chenghui Zhang ................................ 1493

Fast Verification of Memory Consistency for Chip Multi-Processor
Zheng Lv, Hao Chen, Feng Chen, and Yi Lv .................... 1497

Finite Volume Methods for the Second Order Singular Perturbation Problems
Chongnan He ................................................. 1503
FTA Based Runtime Evaluation of System Reliability for Autonomous Unmanned Vehicle ..................................................1507
    Guoqi Li

Geometric Recognitions Models of Fault Characteristics in Mobile Core Network ..................................................1510
    Sulin Pang and Shou Yang Wang

Multiobjective Interaction Programming for Two-Persons .................................................................1515
    Min Jiang, Zhiqing Meng, Xinsheng Xu, Rui Shen, and Gengui Zhou

Multi-user Detection Method for MIMO-OFDM Uplink Transmission ..................................................1520
    Wang Yanli

Off-line Text-independent Writer Identification Using a Mixture of Global and Local Features ..................................................1524
    Yiu-ming Cheung and Junping Deng

Optimization Plan of Using the Arrival and Departure Track in District Station Based on Hybrid Algorithm ..................................................1528
    Feng Tian, Hai Yang Wang, Xiaoping Sun, Jia Liu, and Chuanyun Wang

Qualitative Analysis for a Kind of Predator-Prey Model of Holling III-Function Response with Nonlinear Density Dependent ..................................................1532
    Wei-wei Zheng, Li-gui Luo, and Lei Zhao

Relative Stability of Solution for Hua’s Macroeconomic Model ..................................................1536
    Jing Zhang and Jinjie Zhang

Robust Adaptive Sliding Mode Control Design for a Class of Uncertain Neutral Systems with Distributed Delays ..................................................1539
    Ruliang Wang, Dongmei Gao, and Yanbo Li

Stock Selection Based on Data Clustering Method ..................................................1542
    Ruizhong Wang

Structural Health Monitoring via Dynamic Visualization ..................................................1546
    Peng Sun and Xin Guo

The Application of the Internet of Things in Hainan Tourism Scenic Spot ..................................................1549
    Yuanguai Lin

The Application Study about Lucene in Document Retrieval for Office ..................................................1554
    Daiwen Wu

The BSC Alarm Management System Based on Rough Set Theory in Mobile Communication ..................................................1557
    Chao Deng and Sulin Pang

The Construction and Application of Distance and Open Experimental Platform ..................................................1562
    Yu Jiangfeng and Qi Youju

The Guidance and Control of Small Net-recovery UAV ..................................................1566
    Jiatong Chen and Yong Wang