2009 Fifth International Conference on Information Assurance and Security

(IAS 2009)

Xi’an, China
18-20 August 2009

Volume 1
Pages 1-390
Session A-01: Digital Rights Management (IS15 Based)

A Dynamic Graph Watermark Scheme of Tamper Resistance ................................................................. 3
   XiaoJiang Chen, DingYi Fang, JingBo Shen, Feng Chen, WenBo Wang, and Lu He

Trusted Computing Based Mobile DRM Authentication Scheme ............................................................... 7
   Zhen Yang, Kefeng Fan, and Yingxu Lai

An Authenticating Algorithm with Multi-compression Compatible in DCT Domain ................................................................. 11
   XiaoYuan Yang, Yao Guo, Ke Niu, and Xiang Wu

Audio Digital Signature Algorithm with Tamper Detection ......................................................................... 15
   XiaoYuan Yang, Xiang Wu, and Minqing Zhang

Key Binding Based on Biometric Shielding Functions .................................................................................. 19
   Li Huixian, Wang Man, Pang Liaojun, and Zhang Weidong

A Deep Copy Protection Framework for Electronic Devices within Home .................................................. 23
   Yang Zhan, Haibo Tian, Qingqi Pei, Yueyu Zhang, Yumin Wang, and Weidong Zhang

Attacks on a Universal Designated Verifier Signature Scheme .................................................................. 27
   Li Yanping, Pang Liaojun, and Wang Yuming

Image Enhancement Based on Nonsubsampled Contourlet Transform ......................................................... 31
   Yuxin Ma, Jiancang Xie, and Jungang Luo
Session A-02: Multimedia in Ubiquitous Computing and Security Services (IS05 Based)

Image Watermarking Using Phase-Shifting Digital Holography Embedded in the Wavelet Domain .............................................................................................................................................37
   Mn-Ta Lee, Hsuan T. Chang, and Mu-Liang Wang

A Polynomial Based Key Establishment Scheme for Heterogeneous Sensor Networks .....................................................................................................................................................................41
   Iuon-Chang Lin and Shu-Yan Huang

An Adaptable Threshold Decision Method ............................................................................................................................................................................45
   Meng-Hsiun Tsai, Ming-Hung Wang, Ting-Yuan Chang, Pei-Yan Pai, and Yung-Kuan Chan

Zero Packet Loss Hand-off Mechanism in SIP-Based Wireless Networks .........................................................................................................................................................................................49
   Ching-Lung Chang, Jia-Yi Syu, and Yuan-Sun Chu

A New Authenticated Key Agreement Protocol for Wireless Mobile Networks ..........................................................................................................................................................................................53
   Shin-Jia Hwang and Ming-Jhang Chai

Economical Dental Stereoradiography in Digital Era ..............................................................................................................................................................................57
   Hsien-Huang P. Wu, Shih-Hsin Chang, Ping-Kuo Weng, and Soon-Lin Chen

A Resistant Secret Sharing Scheme ..............................................................................................................................................................................61
   Chin-Chen Chang, Yen-Chang Chen, and Chia-Chen Lin

Session A-03: Image Processing and Intelligent Control (IS16 Based)

A Modified Feature Based Image Watermarking Scheme in NSCT Domain ..............................................................................................................................................................................................67
   Liu Yang, Baolong Guo, and Jianmin Lv

Grounding Grid Corrosion Diagnosis Based on Large Change Sensitivity ..............................................................................................................................................................................71
   Liqiang Liu, Xianjue Luo, Tao Niu, and Kai Wang

Anomalous Payload Detection System Using Analysis of Frequent Sequential Pattern ..............................................................................................................................................................................75
   Jun Ma, Guanzhong Dai, and Jing Zhou

An Enhanced Block Mode Selection Method for Surveillance Video Communication ..............................................................................................................................................................................79
   Jie Jiang, Wei Mo, and Jianmin Lv

The Detection of Bi-frequency Weak Signal Based on Chaos and Correlation ..............................................................................................................................................................................................83
   Wang Mei, Zhang Huiyong, and Yan Yong

Application of Rough Set Theory in Coal Gangue Image Process ..............................................................................................................................................................................................87
   Xian-Min Ma and Che Liang

GOP-Level Transmission Distortion Modeling for Video Streaming over Mobile Networks ..............................................................................................................................................................................................91
   Yu Han, Aidong Men, Kan Chang, and Ziyi Quan

Sinusoidal Signals Pattern Based Robust Video Watermarking in the 3D-CWT Domain ..............................................................................................................................................................................................96
   Cheng Deng, Jie Li, Meng Jia, and Xinbo Gao
Session A-04: Video Coding Schemes

Assessment of Color Video Quality with Singular Value Decomposition of Complex Matrix .................................................................103

Fuqiang Zhang, Junli Li, Gang Chen, and Jiaju Man

Hybrid Video Transcoder for Bitrate Reduction of H.264 Bit Streams ........................................................107

Min Li and Bo Wang

Whole Frame Loss Recovery Algorithm for H.264 Decoders .................................................................................................111

Min Li and Bo Wang

A Frequent-Domain Video Transcoder with Spatial Downscaling for H.264/AVC .........................................................................................115

Bo Wang and Dichen Liu

A Novel Video Shot Segmentation Based on Textural Features .........................................................................................119

Yin Wang, Xiangming Wen, Xinqi Lin, Peizhou He, and Wei Zheng

Octagonal Search Algorithm with Early Termination for Fast Motion Estimation on H.264 ..........................................................123

Zhaopeng Cui, Dujuan Wang, Guang Jiang, and Chengke Wu

A Two-Description Distributed Video Coding .........................................................................................................................127

Anhong Wang, Yao Zhao, and Zhihong Li

Session A-05: Fuzzy Applications

Fuzzy Identity Based Encryption Scheme with Some Assigned Attributes .................................................................133

XiMing Li, Bo Yang, and YuBin Guo

Encrypted Fuzzy Vault Based on Fingerprint .........................................................................................................................137

Feng Quan, Su Fei, and Cai Anni

An Attack Model Based on Both-Branch Fuzzy Logic and Fuzzy Petri Net .........................................................................................141

Qiuqin Lu and Guangqiu Huang

Application of the Fuzzy Entropy Weight in Risk Assessment of the Engineering Project .................................................................145

Xuyan Wu, Huiling Gu, Xujie Hu, and Yuhong Dong

An Adaptive Fuzzy Scheduling and Fuzzy-PID Performance Control Model Being Suitable to Soft Real-Time Systems .........................................................................................149

Xian-Bo He, Li Yang, Xian-hua Zeng, Gang-yuan Zhang, and Xing-qiang Zhao

Fuzzy Intrusion Detection System via Data Mining Technique with Sequences of System Calls ........................................................................154

Mohammad Akbarpour Sekeh and Moh. Aizani Bin Maarof

Application of Particle Swarm Optimization in Fuzzy Neural Networks .........................................................................................158

Qingnian Wang, Kun Yan, Xiaofeng Wan, and Meiling Yuan
Session A-06: System-on-Chip for Signal Processing (IS07 Based)

Full System Simulation and Verification Framework .......................... 165
   Jing-Wun Lin, Chen-Chieh Wang, Chin-Yao Chang, Chung-Ho Chen, Kuen-Jong Lee,
   Yuan-Hua Chu, Jen-Chieh Yeh, and Ying-Chuan Hsiao

Automatic IP Interface Synthesis Supporting Multi-layer Communication Protocols in SoC Designs .................................................. 169
   Yin-Tsung Hwang and Hua-Hsin Luo

Moving Object Tracking Using Symmetric Mask-Based Scheme .................. 173
   Chih-Hsien Hsia, Ding-Wei Huang, Jen-Shiun Chiang, and Zong-Jheng Wu

Hardware/Software Codesign of Resource Constrained Real-Time Systems .................................................. 177
   Chia-Cheng Lo, Jung-Guan Luo, and Ming-Der Shieh

Design and Integration for Background Subtraction and Foreground Tracking Algorithm .................................................. 181
   Tsung-Han Tsai, Chung-Yuan Lin, De-Zhang Peng, and Giua-Hua Chen

Parallel 3-Pixel Labeling Method and its Hardware Architecture Design .................................................. 185
   Shyue-Wen Yang, Ming-Hwa Sheu, Jun-Jie Lin, Chuang-Chun Hu, Tzu-Hsiung Chen,
   and Shau-Yin Tseng

Novel Fast Mode Decision Algorithm for P-Slices in H.264/AVC .................. 189
   Kan Chang, Bo Yang, and Wenhao Zhang

Session A-07: Data Hiding Techniques (IS01 Based)

Majority-Parity-Guided Watermarking for Block-Truncated Images .................. 197
   Jing-Ming Guo and Yun-Fu Liu

Data Hiding in Halftone Images Using Adaptive Noise-Balanced Error Diffusion and Quality-Noise Look Up Table .................................................. 201
   Jing-Ming Guo and Jia-Jin Tsai

Improving the Modified Matrix Encoding on Steganography Method .................................................. 205
   YongSoo Choi and HyoungJoong Kim

Reversible Information Hiding Considering Hierarchical Access Control .................. 209
   Masaaki Fujiyoshi, Seungwu Han, and Hitoshi Kiya

The Reversible Network Cascade Based on Reversible Logic Gate Coding Method .................................................. 213
   Hui Li, Zhijin Guan, Shanli Chen, and Yuxin Chen

Image Compression Algorithm Based on Decreasing Bits Coding .................. 217
   Shengbing Che, Zuguo Che, Haiyang Wang, and Qiangbo Huang

A Digital Watermarking Algorithm for DEM Image Based on Stationary Wavelet Transform .................................................. 221
   He Xiang and Liu Jianjun

Redundant Ridgelet Transform and its Application to Image Processing .................. 225
   Yan Li, Shengqian Wang, and Chengzhi Deng
Session A-08: Digital Rights Management (IS15 Based)

Performance Analysis of Chinese Webpage Categorizing Algorithm Based on Support Vector Machines (SVM) .......................................................... 231
  Xiao Gang and Xie Jiexiang

Research on Improved Algorithm for Chinese Word Segmentation Based on Markov Chain .......................................................... 236
  Pang Baomao and Shi Haoshan

A New Histogram Based Image Watermarking Scheme Resisting Geometric Attacks .......................................................... 239
  Xin-Wei Li, Bao-Long Guo, Lei-Da Li, and Hong-Xin Shen

An Adaptive Digital Watermarking Algorithm Based on Balanced Multi-wavelet .......................................................... 243
  Ming-Xiang Zang, Na Zhang, and Jian-Guo Jiang

An Improved Iris Recognition Method Based on Gray Surface Matching .......................................................... 247
  Dong-Mei Wu and Jiang-Nan Wang

Image Retrieval Based on 2D Histogram of Interest Points .......................................................... 250
  Fan-jie Meng, Bao-long Guo, and Lei Guo

An Improved Fusion Algorithm of the Weighted Features and its Application in Image Retrieval .......................................................... 254
  Mei Wang and Li Wang

An Active Defense Model and Framework of Insider Threats Detection and Sense .......................................................... 258
  Hongbin Zhang, Jianfeng Ma, Yinchuan Wang, and Qingqi Pei

Session A-09: Image Processing and Intelligent Control (IS16)

The Application and Study of Graph Cut in Motion Segmentation .......................................................... 265
  Ye Hou, Bao-long Guo, and Jeng-Shyang Pan

A Dynamic Layering Scheme of Multicast Key Management .......................................................... 269
  Fan Yang, Xiao-ping Li, Qing-kuan Dong, and Yan-ming Liu

Research on 3D Reconstruction Procedure of Marked Points for Large Workpiece Measurement .......................................................... 273
  Zhanli Li and Yuan Wang

Research on Video Information Camouflage Processing Algorithm Based on Pulse Amplitude Modulation .......................................................... 277
  Yang Qiu, Jin Tian, and Liuyu Qian

A New Multiple-Objects Tracking Method with Particle Filter .......................................................... 281
  Long Chen, Bao-long Guo, and Wei Sun

Support Vector Machine Based on Possibility Degrees and Fault Diagnosis .......................................................... 285
  Du Jingyi, Wang Mei, and Cai Wenhao
Optimal Combination of H.264/AVC Coding Tools for Mobile Multimedia
Broadcasting Application ........................................................................................................... 289
    Yu Han, Bo Yang, Kan Chang, and Ziyi Quan

Distributed Video Coding Based on Multiple Description ................................................................... 294
    Hongxia Ma, Yao Zhao, Chunyu Lin, and Anhong Wang

Session A-10: Cryptography and Watermarking
A Watermarking Scheme Based on Two-dimensional Wavelet Filter
Parametrization ............................................................................................................................... 301
    Guosheng Cheng and Jianwei Yang

Watermarking Relational Databases for Ownership Protection Based on DWT ........................................... 305
    Chuanxian Jiang, Xiaowei Chen, and Zhi Li

A Fragile Software Watermarking for Tamper-Proof ........................................................................... 309
    Changle Zhang, Hong Peng, Xianzhong Long, Zheng Pan, and Ying Wu

Curvelet Domain Watermark Detection Using Alpha-Stable Models .................................................. 313
    Chengzhi Deng, Huasheng Zhu, and Shengqian Wang

Nonuniformity Correction Algorithms of IRFPA Based on Radiation Source
Scaling ...................................................................................................................................................... 317
    Enke Li, Shangqian Liu, Shimin Yin, and Xiaoming Fu

The SOBER Family Ciphers Reconfigurable Processing Architecture Design ................................ 322
    Wang Zhiyuan, Huang Jianhua, and Guan Ziming

Webpage Encryption Based on Polymorphic Javascript Algorithm ................................................... 327
    Bai Zhongying and Qin Jiancheng

The Improving of IKE with PSK for Using in Mobile Computing
Environments ........................................................................................................................................ 331
    Dingguo Yu and Nan Chen

Session A-11: Cryptography and its Application (IS04 Based)
Common Friends Discovery with Privacy and Authenticity ............................................................. 337
    Shin-Yan Chiou, Shih-Ying Chang, and Hung-Min Sun

Known Signature Attack of ID-Based Multisignature Schemes ......................................................... 341
    Wu-Chuan Yang and Jhih-Syue Jhou

A Generalization of de Weger’s Method ............................................................................................. 344
    Chien-Yuan Chen, Chih-Cheng Hsueh, and Yu-Feng Lin

New Strategy of Efficient SPA-resistant Exponentiations ............................................................... 348
    Wu-Chuan Yang

Browser-Side Countermeasures for Deceptive Phishing Attack ....................................................... 352
    Huajun Huang, Shaohong Zhong, and Junshan Tan

An Anti-attack Watermarking Based on Synonym Substitution for Chinese Text .................................. 356
    He Lu, Lin JianBin, Li TianZhi, and Fang DingYi
Research on Attack Intention Recognition Based on Graphical Model ..........................................................360
   Wu Peng, Zhigang Wang, and Junhua Chen
Anti-protocol Attacks Digital Watermarking Based on Media-Hash and SVD .............................................364
   Jing-pet Wang, Shui-fa Sun, Ming Jiang, Dan-gui Xie, and Bang-jun Lei

Session A-12: Image Retrieval and Image Analysis (IS06 Based)

Intra-mode Dependent Coding Method for Image Compression .................................................................371
   Yung-Chiang Wei, Jui-Che Teng, and Chien-Wen Chung
Dynamically Constrained One-Bit Transform for Motion Vector Estimation .............................................375
   Fu-Kun Chen, Jui-Che Teng, Yue-Dar Jou, and Wen-Yuan Liao
A Name Recommendation Photo Album Using Probability Neural Network ..............................................379
   Ding-Hrong Chen and Shiang-En Tang
Lung Segmentation for Chest Radiograph by Using Adaptive Active Shape Models ........................................383
   Jiann-Shu Lee, Hsing-Hsien Wu, and Ming-Zheng Yuan
The Application on the Evaluation of Quality of Universities Undergraduate Theory Teaching Work Based on Artificial Neural Network .................................................................387
   Jun-qiao Qi, Chang-long Wang, and Yan-ming Qi
Analysis of One-way Alterable Length Hash Function Based on Cell Neural Network ..................................391
   Qun-ting Yang, Tie-gang Gao, Li Fan, and Qiao-lun Gu
The Sync Tracing Based on Improved Genetic Algorithm Neural Network ...............................................396
   Yuanbin Hou, Chunfeng Song, and Ning Li
Research on Intrusion Detection Based on an Improved SOM Neural Network ............................................400
   Dianbo Jiang, Yahui Yang, and Min Xia

Session A-13: Clustering and Target Detection

Words Clustering Based on Keywords Indexing from Large-scale Categorization Corpora ................................407
   Liu Hua
Research on Active Defence Technology with Host Intrusion Based on K-Nearest Neighbor Algorithm of Kernel .................................................................411
   Xuedou Yu
An Improved Weighted-Feature Clustering Algorithm for K-anonymity ...............................................415
   Lijian Lu and Xiaojun Ye
A New Interacting Multiple Model Algorithm Based on the Unscented Particle Filter ................................419
   Deng Xiaolong and Zhou Pingfang
A New Feature Selection Method for Malcodes Detection .........................................................................423
   Xiaokang Zhang and Jianmei Shuai
A New Fingerprint Sequences Matching Algorithm for Content-Based Copy Detection ...................................................................................................................................................................427
   Rongxian Nie, Guiguang Ding, Jianmin Wang, and Li Zhang
Infrared Small Weak Target Detection via HOSA ...................................................................................................................................................................431
   Gaoyu Zhang
DWT-Based Shot Boundary Detection Using Support Vector Machine ...................................................................................................................................................................435
   Jun Li, Youdong Ding, Yunyu Shi, and Qingyue Zeng

Session A-14: Swarm Intelligence and Data Mining
A Model of Intrusion Prevention Base on Immune ...................................................................................................................................................................441
   Yaping Jiang, Yong Gan, Jianhua Zhou, and Zengyu Cai
New Greedy Algorithm for Computing Double-Base Chains ...................................................................................................................................................................445
   Ming Li and Kunpeng Wang
An Eco-Defending Architecture for Network Security Based on Immunity and Mobile Agents ...................................................................................................................................................................451
   Tongrang Fan, Yan Sun, and Yongbin Zhao
An Improved Genetic Algorithm for Power Grid ...................................................................................................................................................................455
   Youchan Zhu, Xueying Guo, and Jing Li
Swarm Intelligence: Ant-Based Robot Path Planning ...................................................................................................................................................................459
   Jing Zhou, Guan-Zhong Dai, De-Quan He, Jun Ma, and Xiao-Yan Cai
DCT-Based Robust Watermarking with Swarm Intelligence Concepts ...................................................................................................................................................................464
   Hsiang-Cheh Huang, Yueh-Hong Chen, and Guan-Yu Lin
A New Scheme to Privacy-Preserving Collaborative Data Mining ...................................................................................................................................................................468
   Jianming Zhu
Information Security Monitoring System Based on Data Mining ...................................................................................................................................................................472
   Guangjuan Lv, Ruzhi Xu, Xiangrong Zu, and Liwu Deng

Session A-15: Internet Techniques
ID-Based Non-interactive Deniable Authentication Protocol ...................................................................................................................................................................479
   Wei-min Shi
Certificateless One-Way Authenticated Two-Party Key Agreement Protocol ...................................................................................................................................................................483
   Wuping Chen, Lei Zhang, Bo Qin, Qianhong Wu, and Huanguo Zhang
A Secure ID-Based Explicit Authenticated Key Agreement Protocol without Key Escrow ...................................................................................................................................................................487
   Mengbo Hou and Qiuliang Xu
Multi-party Non-repudiation Protocol with Different Message Exchanged ...................................................................................................................................................................491
   Li Yanping and Pang Liaojun
An Improved Scheme of Single Sign-on Protocol ...................................................................................................................................................................495
   Yang Jian
A New Efficient and Strongly Secure Authenticated Key Exchange Protocol ...................................................................................................................................................................499
   Qingfeng Cheng, Guangguo Han, and Chuangui Ma
An Automated Mechanism of Security Test on Network Protocols ..........................................................503  
Yahui Yang, Yunfei Chen, Min Xia, and Juan Ma

An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad Hoc Networks ..............................................................507  
Jian Liu and Fang-min Li

Session B-01: Information Security (IS09 Based)

Zero-Collision RFID Tags Identification Based on CDMA .................................................................513  
Lih-Chyau Wuu, Yen-Ju Chen, Chi-Hsiang Hung, and Wen-Chung Kuo

An Enhanced Remote User Authentication Scheme Providing Mutual Authentication and Key Agreement with Smart Cards .................................................517  
Chun-Ta Li

Security Enhancement of the Authentication Protocol for RFID Systems ...........................................521  
Yung-Cheng Lee, Wen-Chung Kuo, Y.-C Hsieh, and T.-C. Chen

Secure Access Control Scheme of RFID System Application .........................................................525  
Yu-Chih Huang

Paper Study of Embedded System Design Based on RFID Securities ..................................................529  
Ling-feng Shi, Xin-Quan Lai, and Bao-Long Guo

Improvement of an EPC Gen2 Compliant RFID Authentication Protocol .........................................532  
Kuo-Hui Yeh and N.W. Lo

A New Multi-bank E-cash Protocol with Anonymity Control .............................................................536  
Lingling Wang

Practical Quantum No-key Protocol with Identification .....................................................................540  
Yang Wu and Li Yang

Session B-02: Multimedia Processing and Multimedia Interaction (IS10 Based)

Facial Expression Recognition Based on Field Programmable Gate Array ........................................547  
Jzu-Sheng Lin, Shao-Han Liou, Wu-Chih Hsieh, Yu-Yi Liao, HongChao Wang, and QingHua Lan

Analysis and Evaluation of Contrast Enhancement Methods in Digital Images ................................551  
Shen-Chuan Tai, Yi-Ying Chang, Ting-Chou Tsai, and Li-Man Liao

Contrast Enhancement Method Based on Average Luminance with Weighted Histogram Equalization ........................................................................555  
Shen-Chuan Tai, Yi-Ying Chang, Kang-Ming Li, and Ting-Chou Tsai

Application of Averaged Learning Subspace Method in MRI Classification .......................................559  
Chuin-Mu Wang, Jau-An Chen, and Jui-Hsing Chu

Low Bit Rate ROI-Based SAR Image Compression ..............................................................................563  
Xiao-Hong Yuan, Zhao-Da Zhu, and Gong Zhang

Image Retrieval Based on Composite of Mean Shift and Assignment Model ......................................568  
Wenbing Chen, Qi-zhou Li, and Jianwei Yang
A RST Invariant Watermarking Scheme Utilizing Support Vector Machine and Image Moments for Synchronization .......................................................... 572
  Jianzhen Wu

Image Moment Based Registration Scheme Utilizing Support Vector Machine .................................................. 575
  Jianzhen Wu

**Session B-03: Image Engineering and Network Security (IS19 Based)**

A New Adaptive Image Denoising Method Combining the Nonsubsampled Contourlet Transform and Total Variation .......................................................... 581
  Xiaoyue Wu, Baolong Guo, Shengli Qu, and Zhuo Wang

SAR Image Target Recognition Based on Hu Invariant Moments and SVM .................................................. 585
  Fu Yan, Wang Mei, and Zhang Chunqin

Testability Analysis of Grounding Grids Using Network Transformation .................................................. 589
  Tao Niu, Yingjiao Zhang, Debo Zhang, Liqiang Liu, and Xianjue Luo

Research on Algorithm of Digital Filtering Based on Video Information Security ........................................... 593
  Jin Tian, Yang Qiu, and Liuyu Qian

ISAR Imaging of High Speed Moving Targets Based-on Radon Transform .................................................. 597
  Feng Tong-an, He Jin, and Luo Ying

Octa-Log-Polar Fourier Transform for Image Registration .......................................................... 601
  Xian-xiang Wu, Bao-long Guo, and Juan Wang

An Improved Image Encryption Scheme Based on Line Maps .......................................................... 605
  Juan Li, Yong Feng, and Xuqiang Yang

Multiresolution Target Detection in Wavelet Domain for SAR Imagery .................................................. 609
  Xiao-Hong Yuan, Zhao-Da Zhu, and Gong Zhang

**Session B-04: Information Security**

A New Accelerated RC4 Scheme Using “Ultra Gridsec” and “HIMAN” and use this Scheme to Secure “HIMAN” Data .......................................................... 617
  Hisham A. Kholidy and Khaled S. Alghathbar

A New Conic Curve Digital Signature Scheme .......................................................... 623
  Xiang Can and You Lin

A High-efficiency Data Distribution Algorithm in Distributed Storage .................................................. 627
  Xiao-Yuan Yang, Zhen Liu, Wei Zhang, and Dun-Tao Guo

An Approach to Group Decision Making Based on Incomplete Linguistic Preference Relations .......................................................... 631
  Tien-Chin Wang, Shu-Chen Peng, Shu-Chen Hsu, and Juifang Chang

Constructions of Some Difference-Balanced d-form Functions .......................................................... 635
  Tongjiang Yan and Li Hong

A Novel Micropayment Scheme with Complete Anonymity .......................................................... 638
  Xin Zhao, Yuqin Lv, and Wenxin He
Domain Administration of Task-role Based Access Control for Process Collaboration Environments .................................................................643
Yahui Lu and Li Zhang

Session B-05: Anti-attack Schemes and Analysis

A Fast Correlation Attack via Parallel Computing ..........................................................651
Qiong Liu and Yupu Hu
A Database Protection System Aiming at SQL Attack ..........................................................655
Deng Liwu, Xu Ruzhi, Jiang Lizheng, and Lv Guangjuan
Guess and Determine Attack on SOSEMANUK ..................................................................658
Ding Lin and Guan Jie
Algebraic Attack to SMS4 and the Comparison with AES .......................................................662
Wen Ji, Lei Hu, and Haiwen Ou
Number-Theoretic Attack on Lyuu-Wu’s Multi-proxy Multi-signature Scheme .................666
Fanyu Kong and Jia Yu
A New JPEG Resistant Color Image Watermarking Algorithm Based on Quantization Index Modulation ..........................................................669
Nie Jie, Wei Zhiqiang, and Li Zhen
A Modified Run-length Image Data Hiding for High Embedding Capacity .......................673
Rey-Sern Lin and Shang-Wen Hu

Session B-06: Soft Computing and Hybrid Intelligent Approaches in Computer Security (IS18 Based)

Intelligent Clustering with PCA and Unsupervised Learning Algorithm in Intrusion Alert Correlation ........................................................................679
Maheyzah Md Siraj, Mohd Aizaini Maarof, and Siti Zaiton Mohd Hashim
Fuzzy c-Means Sub-Clustering with Re-sampling in Network Intrusion Detection .................................................................683
Anazida Zainal, Den Fairol Samaon, Mohd Aizaini Maarof, and Siti Mariyam Shamsuddin
Hierarchical Takagi-Sugeno Models for Online Security Evaluation Systems ................687
Ajith Abraham, Crina Grosan, Hongbo Liu, and Yuehui Chen
Detecting Insider Attacks Using Non-negative Matrix Factorization ................................693
Jan Platoš, Vaclav Snasel, Pavel Krömer, and Ajith Abraham
Adaptive-Push Peer-to-Peer Video Streaming System Based on Dynamic Unstructured Topology ........................................................................697
Xiaodong Shen, Guiguang Ding, Yizheng Chen, and Jianmin Wang
Evaluation and Simulation on the Performance of DHTs Required by P2PSIP .....................701
Zengming Tian, Xiangming Wen, Wei Zheng, Yong Sun, and Yinbo Cheng
The Research on the Measurement of China Internet Illegal and Harmful Content .................................................................705
Qiang Song and Gang Li
Network Traffic Anomaly Detection Based on Self-Similarity Using HHT and Wavelet Transform ............................ 710
  Xiaorong Cheng, Kun Xie, and Dong Wang

Session B-07: Multimedia Signal Processing for Public Safety and Privacy (IS08 Based)

Privacy Protection for Speech Information ............................................................................................................ 717
  Kazumasa Yamamoto and Seiichi Nakagawa

Improvement of Speaker Vector-Based Speaker Verification ................................................................................ 721
  Naoki Tadokoro, Tetsuo Kosaka, Masaharu Kato, and Masaki Kohda

Acoustic-Based Security System: Towards Robust Understanding of Emergency Shout ........................................ 725
  Hiroaki Nanjo, Takanobu Nishiura, and Hiroshi Kawano

A System for Detecting Unusual Sounds from Sound Environment Observed by Microphone Arrays .................. 729
  Mitsuru Kawamoto, Futoshi Asano, Koichi Kurumatani, and Yingbo Hua

Detection of Abnormal Sound Using Multi-stage GMM for Surveillance Microphone .............................................. 733
  Akinori Ito, Akihito Aiba, Masashi Ito, and Shozo Makino

An Audio Watermarking Method of Resistance Statistics Attack Based on Psychoacoustic Model ....................... 737
  Xiao-li Liu, Shui-fa Sun, Jian-wei Zhu, Ming Jiang, and Dan-gui Xie

Cepstrum-Based Audio Watermarking Algorithm against the A/D and D/A Attacks .............................................. 740
  Xiaoming Zhang and Zhaoyang Yu

Compensating Function of Formant Instantaneous Characteristics in Speaker Identification .................................. 744
  Limin Hou and Juanmin Xie

Session B-08: Image Engineering and Network Security (IS19 Based)

Design of DBA Algorithm in EPON Uplike ............................................................................................................ 751
  Ya-min Wang and Yan Liu

Cramer-Rao Lower Bound for Non-coherent TOA Estimation with Impulse Signal .............................................. 754
  Jie Liu, Xiaoji Liu, and Lin Zheng

Research on Intrinsic Safety Behavior of Inductor-Disconnected-Discharge of Boost DC-DC Converters ............. 758
  Liu Shulin and Li Yan

Study on the Control of a Two-wheeled Unstable Vehicle Based on Sensitivity Analysis ..................................... 762
  Yanzhao Li, Shengli Qu, Jiahui Zhu, and Jianqin Sun
Generalized Analysis Model of Information Security of Computer System Based on Electromagnetic Topology .......................................................... 766
   Jin Tian, Yang Qiu, and Ankun Lin

The Design and Implementation of Security Defense Technology Based on Mandatory Running Control ............................................................. 770
   Liu Jizhen, Wu Kehe, Zhang Tong, and Ma Gang

An Accurate Image Juggling Authentication Algorithm ................................................................. 774
   Jianquan Xie, Qing Xie, and Chunhua Yang

Universal Steganalysis Based on Statistical Models Using Reorganization of Block-based DCT Coefficients .......................................................... 778
   Shaohui Liu, Lin Ma, Hongxun Yao, and Debin Zhao

Author Index - Volume 1
# Table of Contents

**Volume - 2**

### Preface - Volume 2

### Committee Lists - Volume 2

### Session B-09: Security Coding Algorithms and Analysis

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A New Algorithm for Outlier Detection Based on Offset</td>
<td>3</td>
</tr>
<tr>
<td>Yue Zhang, Jie Liu, and Bo Song</td>
<td></td>
</tr>
<tr>
<td>Information Security Solution Decision-Making Based on Entropy Weight</td>
<td>7</td>
</tr>
<tr>
<td>and Gray Situation Decision</td>
<td></td>
</tr>
<tr>
<td>Lin Chen, Li Li, Yong Hu, and Ke Lian</td>
<td></td>
</tr>
<tr>
<td>Quantum Secure Direct Communication Based on Partially Entangled States</td>
<td>11</td>
</tr>
<tr>
<td>Xin-yuan Yang, Zhi Ma, Xin Lü, and Hong-xin Li</td>
<td></td>
</tr>
<tr>
<td>A Multi-view Nonlinear Active Shape Model Based on 3D Transformation</td>
<td>15</td>
</tr>
<tr>
<td>Shape Search</td>
<td></td>
</tr>
<tr>
<td>Yi Faling, Xiong Wei, Huang Zhanpeng, and Zhao Jie</td>
<td></td>
</tr>
<tr>
<td>Analysis the Properties of TLS Based on Temporal Logic of Knowledge</td>
<td>19</td>
</tr>
<tr>
<td>Lv Chao, Li Hui, and Ma Jianfeng</td>
<td></td>
</tr>
<tr>
<td>f8 Keystream Generator with SMS4 as Core Algorithm</td>
<td>23</td>
</tr>
<tr>
<td>Wang Yingsong and Chen Wei</td>
<td></td>
</tr>
<tr>
<td>Waveform Analysis Mathematic Based on Ultrasonic Displacement</td>
<td>27</td>
</tr>
<tr>
<td>Measurement</td>
<td></td>
</tr>
<tr>
<td>Wang Yuhui and Dai Ju</td>
<td></td>
</tr>
<tr>
<td>Research on Security Architecture for Defending Insider Threat</td>
<td>30</td>
</tr>
<tr>
<td>Hui Wang, Heli Xu, Bibo Lu, and Zihao Shen</td>
<td></td>
</tr>
</tbody>
</table>
Session B-10: Cryptanalysis and its Application

On Security Notions for Verifiably Encrypted Signature .................................................................37
   Xu An Wang, Xiaoyuan Yang, and Qingquan Peng

Secure Disk with Authenticated Encryption and IV Verification ..................................................41
   Fangyong Hou, Nong Xiao, Fang Liu, and Hongjun He

Non-interactive Evaluation of Encrypted Elementary Functions ...............................................45
   Liang Chen, Chengmin Gao, and Yong Xu

Cryptanalysis of a Knapsack Public Key Cryptosystem .................................................................49
   Baocang Wang, Hui Liu, and Yupu Hu

A New Knapsack Public-Key Cryptosystem ..................................................................................53
   Weidong Zhang, Baocang Wang, and Yupu Hu

Forward-Secure Certificate-Based Encryption ..............................................................................57
   Yang Lu and Jiguo Li

Image Encryption with Discrete Fractional Cosine Transform and Chaos ..................................61
   Lin Zhang, Jianhua Wu, and Nanrun Zhou

Cryptoanalysis of Two Signcryption Schemes ..............................................................................65
   Jianhong Zhang and Qin Geng

Session B-11: 3D Model Retrieval and Data Hiding (IS12 Based)

A Novel Multiple Description Coding Frame Based on Reordered DCT ......................................71
   Lin-Lin Tang, Zhe-Ming Lu, and Fa-Xin Yu

A CELP-Speech Information Hiding Algorithm Based on Vector Quantization .......................75
   Ji-Xin Liu, Zhe-Ming Lu, and Hao Luo

Video Identification Using Spatio-temporal Salient Points ..........................................................79
   Yue-nan Li and Zhe-ming Lu

A Novel Approach for Audio Watermarking ................................................................................83
   Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Akram M. Zeki, and Pritheega Magalingam

Efficient Certificate-Based Signature Scheme ..............................................................................87
   Yang Ming and Yumin Wang

A Comparative Statistical Analysis of Pseudorandom Bit Sequences .........................................91
   Rashidah Kadir and Mohd Aizaini Maarof

Small Moving Infrared Target Detection Algorithm under Low SNR Background .......................95
   Kai Wang, Yan Liu, and Xiaowei Sun

Collusion-Resilient Fingerprinting Using Cropping and Subsampling ....................................98
   Yueh-Hong Chen and Hsiang-Cheh Huang
Session B-12: Internet Security and Electronic Commerce Security (IS13 Based)

Privacy Protection in On-line Shopping for Electronic Documents ................................................................. 105
  Yu-Chi Chen, Gwooba Horng, and Chang-Chin Huang
A Low-cost RFID Authentication Protocol with Location Privacy Protection .................................................. 109
  Yu-Yi Chen, Jun-Chao Lu, Shin-I Chen, and Jinn-Ke Jan
A Real-Time Selective Video Encryption Using Context-Key Control ............................................................ 114
  Hung-Min Sun and Muh-Chyi Leu
Ideal Perfect Multilevel Threshold Secret Sharing Scheme .................................................................................. 118
  Changlu Lin, Lein Harn, and Dingfeng Ye
Implementation of an Electronic Voting System with Contactless IC Cards for Small-Scale Voting .................. 122
  Chung-Huang Yang, Shih-Yi Tu, and Pei-Hua Yen
Access Log Generator for Analyzing Malicious Website Browsing Behaviors .................................................. 126
  Chu-Hsing Lin, Jung-Chun Liu, and Ching-Ru Chen
An Extensible and Virtualization-Compatible IDS Management Architecture .................................................. 130
  Sebastian Roschke, Feng Cheng, and Christoph Meinel
Deadlock Detection Based on Resource Allocation Graph .................................................................................. 135
  Qinqin Ni, Weizhen Sun, and Sen Ma

Session B-13: Network Security

Exploiting RFC2828 as a Domain Vocabulary for Identifying IT Security Literature .................................................. 141
  Lidong Wang and Liping Qian
The Research of Simulation for Network Security Based on System Dynamics .................................................. 145
  Hong-shan Kong, Ming-qing Zhang, Jun Tang, and Chang-yuan Luo
Network Security Situation Awareness Using Exponential and Logarithmic Analysis ...................................... 149
  Tan Xiaobin, Qin Guihong, Zhang Yong, and Liang Ping
Security Threats and Countermeasures for Intra-vehicle Networks ................................................................. 153
  David Wampler, Huirong Fu, and Ye Zhu
W-Aegis: A Propagation Behavior Based Worm Detection Model for Local Networks ...................................... 158
  Zhanyong Tang, Rui Qi, Dingyi Fang, and Yangxia Luo
Research on Early Warning for Worm Propagation Based on Area-Alert-Level .............................................. 163
  Li-na Zhu, Chao-yi Sun, and Li Feng
Modeling and Analyzing the Spread of Worms with Bilinear Incidence Rate ............................................... 167
  Chen Junhua and Wei Shengjun
Modeling the Co-evoluation DNS Worms and Anti-worms in IPv6 Networks ............................................... 171
  P. Kammis, T. Komninos, and Y.C. Stamatiou
Session B-14: System Design and Implementation III

Multimodal Biometric Recognition Based on Complex KFDA ................................................................. 177
   Zhifang Wang, Qiong Li, Xiamu Niu, and Christoph Busch
An Approach to Checking SOC Timing Safety .................................................................................... 181
   Zhenjun Du and Rong Chen
Research on System of Chinese Document Copy Detection .......................................................... 185
   Yuzhu Cheng, Chunrong Qiu, Weiqi Tang, and Wenda Deng
Membership-Based Access Control for Trust Negotiation in Open Systems ................................ 189
   Ruo-Fei Han, Hou-Xiang Wang, Yu-Hua Wang, and Kai-Ling Zuo
ECC-Cache: A Novel Low Power Scheme to Protect Large-Capacity L2 Caches from Transient Faults ................................................................. 193
   Guanghui Liu
Secure Constructing Bluetooth Scatternet Based on BTCP ......................................................... 200
   Xin Yu and YuPing Wang
Space Time Block Coded MIMO System with Redundant Antennas ........................................ 204
   Feng Wang, Xia Liu, and Marek E. Bialkowski
RSA/Shift Secured IFFT/FFT Based OFDM Wireless System .................................................. 208
   D. Rajaveerappa and Abdelsalam Almarimi

Session B-15: Image Processing and its Applications

Infrared Face Recognition Based on Radiant Energy and Curvelet Transformation ................................................. 215
   Zhihua Xie, Shiqian Wu, Guodong Liu, and Zhijun Fang
Fast Fractal Image Coding Using Ambient-Cross Sum of Normalized Block ........................................ 219
   Gaoping Li
Lossy Compression of CFA Image Based on Multiwavelet Packet ............................................ 223
   Jing Zheng, QiGui Zhang, and XueMei Zhang
An Improved SPECK Image Coding Algorithm ............................................................................. 227
   Baojun Han and Yan Liu
A Robust Watermark Algorithm for JPEG2000 Images ............................................................ 230
   Hai-ying Gao, Guo-qiang Liu, Xu Li, and Yin Xu
A Novel Method for Plane Array Infrared Image to Detect Point Target ..................................... 234
   Che Hong and Sun Longhe
A New Image Restoration Algorithm Based on Variational Derivative .................................... 241
   Wenjuan Zhang and Weibin Zhang
Visibility Estimation Based on Mean Shift ........................................................................................ 245
   Wenbing Chen, Xiaolei Zhang, and Jianwei Yang
Session C-01: Internet Security and Electronic Commerce Security (IS03 Based)

Detecting DoS and DDoS Attacks by Using an Intrusion Detection and Remote Prevention System .................................................. 251
  Fang-Yie Leu and Zhi-Yang Li

Detecting DoS and DDoS Attacks Using Chi-Square .................................................. 255
  Fang-Yie Leu and Chia-Chi Pai

Hierarchical Key Agreement Protocols in Group-User Systems ................................).. 259
  Shiuh-Jeng Wang, Yuh-Ren Tsai, Chien-Chih Shen, and Pin-You Chen

Insider DoS Attacks on Epidemic Propagation Strategies of Network Reprogramming in Wireless Sensor Networks .................................... 263
  Yu Zhang, Xing She Zhou, Yee Wei Law, and Marimuthu Palaniswami

Joint Entropy Analysis Model for DDoS Attack Detection ......................................... 267
  Hamza Rahmani, Nabil Sahli, and Farouk Kammoun

Risk Assessment Model on the Internal Corporate Governance Based on the SPA ................................................................. 272
  Jibin Ma, Huiling Gu, Yonghao Sun, and Xujie Hu

Appraisal Model of MIS in Enterprises Based on the Unascertained Measurement ................................................................. 277
  Xuyan Wu, Huiling Gu, Xujie Hu, and Yuhong Dong

Identity Based Multi-proxy Multi-signcryption Scheme for Electronic Commerce ................................................................. 281
  Ying Sun, Chunxiang Xu, Fagen Li, and Yong Yu

Session C-02: Security in Sensor Networks (IS13 Based)

An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks .................. 287
  Xiaqing Li, Hui Li, Jianfeng Ma, and Weidong Zhang

Distributed Event-Triggered Trust Management for Wireless Sensor Networks ................. 291
  Sibo Liu, Liaojun Pang, Qingqi Pei, Hua Ma, and Qingquan Peng

A Novel Biometric-Based Authentication Scheme with Privacy Protection ................... 295
  Li Huixian and Pang Liaojun

Towards Provably Secure On-demand Source Routing in MANET .......................... 299
  Lqiang Mao, Jianfeng Ma, and Xuewen Dong

Research on Integration of Safety Analysis in Model-Driven Software Development ..................... 303
  Chen Feng, Li Weihua, Fang Dingyi, and Chen Xiaojiang

An Authentication Protocol Applied to RFID Security Systems .......................... 307
  Xiaqing Gong, Yi Wang, Hui Li, and Jian He

MRDWA: Multi-role Dynamic Weighting Aggregation Algorithm in Event Driven Wireless Sensor Networks .................. 311
  Ying Chen, Jian Shu, Hong Liu, Linlan Liu, and Jiajie Gong
An Identification Method for Transient Capacitive Current of Distribution Network by ICMAC

Jianwen Zhao and Yuanbin Hou

Session C-03: Identity Validation and Internet Protocol

Development of a Java-Oriented Software General Component Library

Han Xiao, Zu-xun Zhang, Qiang Wang, and Hua-liang Hu

Two Efficient Fragile Web Page Watermarking Schemes

Peng Sun and Hongtao Lu

Researches on Integrating Database Access Control and Privacy Protection

Yonghong Yu

A New Source Address Validation Scheme Based on IBS

Ning-ning Lu, Hua-chun Zhou, and Hong-ke Zhang

Shibboleth Access for Resources on the National Grid Service (SARoNGS)

Xiao Dong Wang, Mike Jones, Jens Jensen, Andrew Richards, David Wallom, Tiejun Ma, Robert Frank, David Spence, Steven Young, Claire Devereux, and Neil Geddes

Defending against UDP Flooding by Negative Selection Algorithm Based on Eigenvalue Sets

Rui Xu, Wen-li Ma, and Wen-ling Zheng

Intrusion Detection Based on One-class SVM and SNMP MIB Data

Cui-Mei Bao

Research on Gravity-Based Anomaly Intrusion Detection Algorithm

Baoyi Wang, Ranran Jin, Shaomin Zhang, and Xiaomin Zhao

Session C-04: Image Clustering and Feature Analysis

Image Retrieve Based on Primary Clusters

Wenbing Chen, Jianwei Yang, and Wangwei

An Effective Texture Spectrum Descriptor

Xiaosheng Wu and Junding Sun

Texture Feature Analysis on Erosion and Wear in Artillery Chamber

Xiao-ning Fu, En-ke Li, and Wen-jing Gao

Image Retrieval Based on Character-Matching Technology

Zhao Shan and Liu Jing

Microarray Image Segmentation Using Region Growing Algorithm and Mathematical Morphology

Ping Ye and Guirong Weng

A Study on the Algorithm Based on Image Color Correlation Mining

Yongyue Chen and Huosong Xia

An Improving Technique of Color Histogram in Segmentation-based Image Retrieval

Zhenhua Zhang, Wenhui Li, and Bo Li
2-Level-Wavelet-Based License Plate Edge Detection ................................................................. 385
  Ming-Kan Wu, Jing-Siang Wei, Hao-Chung Shih, and Chian C. Ho

**Session C-05: System Design and Implementation**

Bearings Fault Diagnosis Based on the Optimal Impulse Response Wavelet ........................................... 391
  Dan Zhang and Wentao Sui

A Digital Certificate Application Scheme in Content Protection System
for High Definition Digital Interface ................................................................................................. 395
  Kefeng Fan, Subing Zhang, and Wei Mo

Research on Equiponderant Forwarding within Multi-nexthop Interfaces .................................................. 399
  Ning-ning Liang and Xuan-yong Zhu

One-way Hash Function Construction Based on Conservative Chaotic Systems ........................................ 402
  Qing-hua Zhang, Han Zhang, and Zhao-hui Li

Resistance DPA of RSA on Smartcard ................................................................................................... 406
  Ji-fang Jin, Er-hong Lu, and Xian-wei Gao

Emergency Command System for Geologic Disasters Prevention ......................................................... 410
  Wenbiao Peng, Chaojun Yan, Xinqiong Liu, and Lihua Deng

Study on Ultrasonic Ranging System Design ......................................................................................... 414
  Lihua Deng

Interactive Visualisation of 3D City Models Based on Adaptive Streaming of 3D-GIS Data ................. 417
  Zhenping Zhang, Jitao Fang, and Runhuan Jing

**Session C-06: Security in Sensor Networks (IS13 Based)**

A New Hybrid Routing Protocol in Heterogeneous Wireless Networks ....................................................... 423
  Yulong Shen, Qijian Xu, Zuoshun Wu, Hao Yin, and Jianfeng Ma

Layer Key Management Scheme on Wireless Sensor Networks .............................................................. 427
  Qingqi Pei, Lei Wang, Hao Yin, Liaojun Pang, and Hong Tang

C and M: A New Network Coding Scheme for Wireless Networks ........................................................ 432
  Xiaoyan Zhu, Hao Yue, and Yumin Wang

Range-Free Fast and Rough Nodes Localization Algorithm in Wireless Sensor Networks ....................... 437
  Wang Mei, Sun Xiaochuan, and Zheng Hao

Information Security Wireless Sensor Grid .............................................................................................. 441
  Li Mingming, Li Baiping, Li Wei, and Chen Lei

An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks ......................... 446
  Chen Chen, Li Hui, Qingqi Pei, Lv Ning, and Peng Qingquan

H2S: A Secure and Efficient Data Aggregative Retrieval Scheme in Unattended Wireless Sensor Networks ......................................................................................................................... 450
  Wei Ren, Yi Ren, and Hui Zhang
Session C-07: E-commerce and E-payment Security (IS14 Based)

A Parity Check Node Synchronization Based Method for Solving Phase Ambiguity Problem in DVB-S Systems ................................................................. 463

Jielin Fu and Yongjun Tang

Security Analysis of the Kerberos Protocol Using BAN Logic ........................................ 467

Kai Fan, Hui Li, and Yue Wang

The Testing and Evaluating System for the Security Operating System Based on the Mechanism of Keyword-Driven ............................................................... 471

Liu Xing, Li Yan, Cai Mian, and Guo Ying

An Identity-Based Authentication Model for Mobile Agent ............................................. 475

Yike Yu, Xuefeng Zheng, Mingde Zhang, and Qingguo Zhang

Performance Analysis of Analog LMS Multiuser Receiver in Transmitted-Reference UWB System .......................................................... 479

Lin Zheng, Wei Ge, and Hongbing Qiu

E-government Security Management: Key Factors and Countermeasure ............................. 483

Jin-fu Wang

A Role and Activity Based Access Control Model for University Identity and Access Management System .............................................................. 487

Shuliang Zheng, Dongxing Jiang, and Qixin Liu

History and Future Information Based Trust Model in C2C E-commerce ............................. 491

Shaomin Zhang, Xiayan Zhang, and Baoyi Wang

Session C-08: Image Filtering and its Application

A Variational Model Combining Curvelet Shrinkage and Nonlinear Anisotropic Diffusion for Image Denoising ................................................................. 497

Weibin Zhang and Wenjuan Zhang

Image De-noising Based on Nonlocal Diffusion Tensor ................................................. 501

Han Yu

A Joint Multiscale Algorithm with Auto-adapted Threshold for Image Denoising ................................................................. 505

Jin He, Yinpei Sun, Ying Luo, and Qun Zhang

A New Scheme for Multisensor Image Fusion System .................................................. 509

Liu Weiguang, Wang Wengi, and Cui Jiangtao

Nonlocal Curvature-Driven Diffusion Model for Image Inpainting .................................. 513

Li li and Han Yu

Adaptive Spatially Postprocessing Technique to Remove Blocking Artifacts for DCT Coded Image ................................................................. 517

Jin Wang, Heechang Kim, Jongho Kim, and Jechang Jeong
Session C-09: System Design and Implementation (II)

Organizational Barriers to the Implementation of Security Engineering .......................................................... 527
   Bryan Stewart Cline
National Information Infrastructure Security and Cyber Terrorism in the Process of Industrializations .......................................................... 532
   Yanzhao Li
A Support Vector Machines Security Assessment Method Based on Group Decision-Marking for Electric Power Information System .......................................................... 536
   Xiaorong Cheng, Yan Wei, and Xin Geng
Threats to Health Information Security .............................................................................................................. 540
   Ganthan Narayana Samy, Rabiah Ahmad, and Zuraini Ismail
An Intrusion Detection System for Network Storage Based on System Calls .......................................................... 544
   Li-zhong Geng and Hui-bo Jia
The Method of Equalization Based on Iterative Interference Cancellation for SCCPM System .......................................................... 548
   Zhao Wusheng, Fu Yongqing, and Han Zhixue
The Research of NULL Convention Logic Circuit Computing Model Targeted at Block Cipher Processing .......................................................... 552
   Yalei Cui and Zibin Dai
Dynamic Behavior of SIS Epidemic Model with Feedback on Regular Lattic .......................................................... 556
   Damin Zhang and Shaohong Cai

Session C-10: Network Security

A Novel Distributed Single Sign-On Scheme with Dynamically Changed Threshold Value .......................................................... 563
   Shangping Zhong, Xiangwen Liao, Xue Zhang, and Jingqu Lin
Building Trust Territory in Ad Hoc Networks .............................................................................................................. 567
   Yuan Bai, Xing Zhang, and Sun Bin
Cost-Benefit Analysis of China’s Internet Content Regulation .............................................................................................................. 571
   Qiang Song and Gang Li
Dynamic Behavior of SIRS Model with Feedback on Complex Networks .......................................................... 576
   Damin Zhang and Shaohong Cai
Position Verification in Multi-hop Vehicular Networks .............................................................................................................. 580
   Deepa Susan Rajan, Chetan Yeole, Harsha Nakade, Huirong Fu, and Ye Zhu
Efficient Protection Scheme for SVC Content Based on Network Coding .............................................................................................................. 585
   Ji Lu, Song Xiao, and Chengke Wu
Application of Bloom Filter for GTP Stateful Inspection in Network Processor .......................................................... 589
   ZhenYu Liu, Weijun Li, and Yue Lai
Session C-11: Watermarking Techniques, Steganography, and Visual Cryptography

An Effective Lossless Hiding Technique Based on Reversible Contrast Mapping and Histogram Embedding Methods ................................................................. 599
Tzu-Chuen Lu and Ying-Hsuan Huang
A High Quality Reversible Data Hiding Method Using Interpolation Technique ......................................................................................................................... 603
Chyuan-Huei Thomas Yang and Chun-Hao Hsu
Reversible Steganography Based on Side Match and Hit Pattern for VQ-Compressed Images ........................................................................................................... 607
Cheng-Hsing Yang, Cheng-Ta Huang, and Shih-Jeng Wang
A High Embedding Efficiency Steganography Scheme for Wet Paper Codes ................................................................................................................................. 611
Zhao-Xia Yin, Chin-Chen Chang, and Yan-Ping Zhang
A Block Feature Correlation Based Image Watermarking for Tamper Detection Using Linear Equation ........................................................................................................ 615
Chin-Feng Lee, Kuo-Nan Chen, Chin-Chen Chang, and Meng-Cheng Tsai
Prediction-Based Watermarking Schemes for DCT-Based Image Coding ................................................................................................................................. 619
Jing-Ming Guo and Chia-Hao Chang
Human Visual System Based Watermarking for Color Images ................................................................................................................................. 623
Kuo-Cheng Liu
Universal Steganalysis to Images with WBMC Model ................................................................................................................................. 627
Xiaoyuan Yang, Shifeng Wang, and Jia Liu

Session C-12: E-commerce and E-payment Security (IS14 Based)

A New Abuse-Free Fair Electronic Payment Protocol ................................................................................................................................. 633
Kai Fan, Yue Wang, and Hui Li
Action-Based Access Control for Web Services ................................................................................................................................. 637
Fenghua Li, Wei Wang, Jianfeng Ma, and Haoxin Su
A Provably Secure Certificateless Blind Signature Scheme ................................................................................................................................. 643
Xiaoyuan Yang, Zhongyin Liang, Ping Wei, and Junwei Shen
Research on Model of Trust Degrees for PKI ................................................................................................................................. 647
Mingde Zhang, Xuefeng Zheng, Wensheng Yang, Shuwang Lv, and Qingguo Zhang
Information Security Routing Protocol in the WSN ................................................................................................................................. 651
Li Wei, Chen Ming, and Li Mingming
Proxy Re-encryption Scheme Based on SK Identity Based Encryption ................................................................................................................................. 657
Xu An Wang and Xiaoyuan Yang
Analysis and Improvement of a Proxy Blind Multi-signature Scheme without a Secure Channel ................................................................................................................................. 661
Ying Sun, Chunxiang Xu, Qi Xia, and Yong Yu
Detecting Stepping-Stone Intruders with Long Connection Chains ............................................. 665
   Wei Ding, Matthew J. Hausknecht, Shou-Hsuan Stephen Huang, and Zach Riggle

Session C-13: Hybrid Techniques

An Optimal Blind Signature Padding with Message Recovery ..................................................... 673
   Jingran Wang and Haifeng Qian
Windows Memory Analysis Based on KPCR .................................................................................. 677
   Ruichao Zhang, Lianhai Wang, and Shuhui Zhang
An Efficient Hierarchical Group Key Management Scheme Based on Orthogonal Vectors .......... 681
   Jing Wang and Xiaola Lin
A Method for Accessing Trusted Services Based on Service-Oriented Architecture .................. 685
   Xin Yu and Yu Bai
Research on Quantitative Evaluation for Integrity ......................................................................... 689
   Lihua Yin and Yunchuan Guo
Research on New Classification Methods of Remote Sensing of Mass Ingredient without Vegetation of Hei Shan Gorge in Yellow River Basin ......................................................... 693
   Shudong Wang and Xiaohua Wang
A Rapid Algorithm and its Implementation for Modular Inversion ............................................... 697
   Baiwen Fu
Optimal Information Rates of Novel Graph Based Access Structures ........................................... 701
   Mingkun Yang

Session C-14: Security Applications

Boosting Graph Embedding with Application to Facial Expression Recognition ................................ 707
   Lei Xiong, Duyan Bi, Xu Zhou, and Shiping Ma
Application and Research of Mobile E-commerce Security Based on WPKI ................................. 711
   Feng Tian, Xiao-bing Han, and Ying Wei
A Performance Evaluation of Security Mechanisms for Web Services ........................................ 715
   Bachar Alrouh and Gheorghita Ghinea
Remark on Yu et al.’s Online/Offline Signature Scheme in CT-RSA 2008 .................................... 719
   Xiao-Long Ma, Zhi-Wei Wang, Li-Ze Gu, and Yi-xian Yang
Towards Secure Content Based Dissemination of XML Documents .......................................... 721
   Mohammad Ashiqur Rahaman, Henrik Plate, Yves Roudier, and Andreas Schaad
Reducing Specular Reflection Components of Chrome-Plated Surface with Varying Light Direction ... 725
   Li Chang Jiang, Zhong Zhang, Tetsuo Miyake, Takashi Imamura, and Hisanaga Fujiwa
Design of Fault Diagnosis System of FPSO Production Process Based on MSPCA .................... 729
   Qiang Gao, Miao Han, Shu-liang Hu, and Hai-jie Dong
Self-selecting Sub-secret Keys Sharing Scheme Based on Polynomials over Elliptic Curve ................................................................. 734

Wang Caimei and Li Zhengmao

Session C-15: System Design and Implementation (IV)

A Robust Vehicle Tracking Approach Using Mean Shift Procedure .......................................................... 741
Huan Shen, Shun Ming Li, Jian Guo Mao, Fang Chao Bo, Fang Pei Li, and Hua Peng Zhou

Augmented Addition Operation of Conic Curves over Ring Zn .......................................................... 745
Guo-jing Li and Tao Wen

Implementing and Testing Producer-Consumer Problem Using Aspect-Oriented Programming .......................................................... 749
Yang Zhang, Jingjun Zhang, and Dongwen Zhang

Soft DSP Design Methodology of Face Recognition System on Nios II Embedded Platform .......................................................... 753
Hao-Chung Shih and Chian C. Ho

Threats Identification in Healthcare Information Systems Using Genetic Algorithm and Cox Regression .......................................................... 757
Rabiah Ahmad, Ganthan Narayana Samy, Nazulha Khilwani Ibrahim, Peter A. Bath, and Zuraini Ismail

Scanning Task Scheduling Strategy in Distributed Vulnerability Detection System .......................................................... 761
Baoyi Wang, Jing Li, Shaomin Zhang, and Xueying Guo

Hierarchical Distributed Alert Correlation Model .......................................................... 765
Donghai Tian, Hu Changzhen, Yang Qi, and Wang Jianqiao

Study on Centralized Authorization Model Supporting Multiple Access Control Models .......................................................... 769
Shaomin Zhang, Haiyan Zhang, and Baoyi Wang

Author Index - Volume 2