

IEICE TRANSACTIONS

O-122-2-1
月 v.96A
刊 n.6

on Fundamentals of Electronics, Communications and Computer Sciences

■ *Special Section on Discrete Mathematics and Its Applications*

■ *Special Section on Circuit, System, and Computer Technologies*

Special Section on Discrete Mathematics and Its Applications

1023 FOREWORD Hisashi KOGA

PAPERS

- 1024 On the Zeta Function of a Periodic-Finite-Type Shift Akiko MANADA and Navin KASHYAP
- 1032 A Compact Encoding of Rectangular Drawings with Edge Lengths
..... Shin-ichi NAKANO and Katsuhisa YAMANAKA
- 1036 Partitioning Trees with Supply, Demand and Edge-Capacity
..... Masaki KAWABATA and Takao NISHIZEKI
- 1044 A Small-Space Algorithm for Removing Small Connected Components from a Binary Image
..... Tetsuo ASANO and Revant KUMAR
- 1051 A Linear-Time Algorithm for Constructing a Spanning Tree on Circular Trapezoid Graphs
..... Hirotoishi HONMA, Yoko NAKAJIMA, Haruka AOSHIMA, and Shigeru MASUYAMA
- 1059 Ranking and Unranking of Non-regular Trees in Gray-Code Order
..... Ro-Yu WU, Jou-Ming CHANG, An-Hang CHEN, and Ming-Tat KO
- 1066 Reporting All Segment Intersections Using an Arbitrary Sized Work Space
..... Matsuo KONAGAYA and Tetsuo ASANO
- 1072 Time-Optimal Gathering Algorithm of Mobile Robots with Local Weak Multiplicity Detection in Rings
..... Tomoko IZUMI, Taisuke IZUMI, Sayaka KAMEI, and Fukuhito OOSHITA
- 1081 Root Computation in Finite Fields Ryuichi HARASAWA, Yutaka SUEYOSHI, and Aichi KUDO
- 1088 Characterization of Strongly Secure Authenticated Key Exchanges without NAXOS Technique
..... Atsushi FUJIOKA
- 1100 Leakage-Resilience of Stateless/Stateful Public-Key Encryption from Hash Proofs
..... Manh Ha NGUYEN, Kenji YASUNAGA, and Keisuke TANAKA
- 1112 Generic Construction of Two-Party Round-Optimal Attribute-Based Authenticated Key Exchange
without Random Oracles Kazuki YONEYAMA
- 1124 One-Round Authenticated Key Exchange with Strong Forward Secrecy in the Standard Model against
Constrained Adversary Kazuki YONEYAMA
- 1139 id-eCK Secure ID-Based Authenticated Key Exchange on Symmetric and Asymmetric Pairing
..... Atsushi FUJIOKA, Fumitaka HOSHINO, Tetsutaro KOBAYASHI, Koutarou SUZUKI,
Berkant USTAOG̃LU, and Kazuki YONEYAMA
- 1156 Methods for Restricting Message Space in Public-Key Encryption
..... Yusuke SAKAI, Keita EMURA, Goichiro HANAOKA, Yutaka KAWAI, and Kazumasa OMOTE

(continued over leaf)

LETTERS

- 1169 On the Security of the Verifiably Encrypted Signature Scheme of Boneh, Gentry, Lynn and Shacham Revisited Bennian DOU
1171 Message and Key Substitution Attacks on Verifiably Encrypted Signature Schemes Bennian DOU

Special Section on Circuit, System, and Computer Technologies

- 1173 FOREWORD Qi-Wei GE

PAPERS

- 1174 Floorplanning and Topology Synthesis for Application-Specific Network-on-Chips
..... Wei ZHONG, Song CHEN, Bo HUANG, Takeshi YOSHIMURA, and Satoshi GOTO
- 1185 LDR Image to HDR Image Mapping with Overexposure Preprocessing
..... Yongqing HUO, Fan YANG, Vincent BROST, and Bo GU
- 1195 Joint Feature Based Rain Detection and Removal from Videos
..... Xinwei XUE, Xin JIN, Chenyuan ZHANG, and Satoshi GOTO
- 1204 Bidirectional Local Template Patterns: An Effective and Discriminative Feature for Pedestrian Detection
..... Jiu XU, Ning JIANG, and Satoshi GOTO
- 1214 A Method of Data Embedding and Extracting for Information Retrieval Considering Mobile Devices
..... Mitsuji MUNAYASU, Hiroshi KUDO, Takafumi SHONO, and Yoshiko HANADA
- 1222 A Design of High Performance Parallel Architecture and Communication for Multi-ASIP Based Image Processing Engine
..... Hsuan-Chun LIAO, Mochamad ASRI, Tsuyoshi ISSHIKI, Dongju LI, and Hiroaki KUNIEDA
- 1236 Sensor Scheduling Algorithms for Extending Battery Life in a Sensor Node
..... Qian ZHAO, Yukikazu NAKAMOTO, Shimpei YAMADA, Koutaro YAMAMURA, Makoto IWATA, and Masayoshi KAI
- 1245 An Image Trading System Using Amplitude-Only Images for Privacy- and Copyright-Protection
..... Shenchuan LIU, Masaaki FUJIYOSHI, and Hitoshi KIYA
- 1253 A Drift-Constrained Frequency-Domain Ultra-Low-Delay H.264/SVC to H.264/AVC Transcoder with Medium-Grain Quality Scalability for Videoconferencing Lei SUN, Zhenyu LIU, and Takeshi IKENAGA
- 1264 Write Control Method for Nonvolatile Flip-Flops Based on State Transition Analysis
..... Naoya OKADA, Yuichi NAKAMURA, and Shinji KIMURA
- 1273 Content-Aware Write Reduction Mechanism of 3D Stacked Phase-Change RAM Based Frame Store in H.264 Video Codec System
..... Sanchuan GUO, Zhenyu LIU, Guohong LI, Takeshi IKENAGA, and Dongsheng WANG
- 1283 A High-Speed Trace-Driven Cache Configuration Simulator for Dual-Core Processor L1 Caches
..... Masashi TAWADA, Masao YANAGISAWA, and Nozomu TOGAWA
- 1293 Bayesian Theory Based Adaptive Proximity Data Accessing for CMP Caches
..... Guohong LI, Zhenyu LIU, Sanchuan GUO, and Dongsheng WANG
- 1306 An Integrated Hole-Filling Algorithm for View Synthesis
..... Wenxin YU, Weichen WANG, Minghui WANG, and Satoshi GOTO
- 1315 Facial Image Super-Resolution Reconstruction Based on Separated Frequency Components
..... Hyunduk KIM, Sang-Heon LEE, Myoung-Kyu SOHN, Dong-Ju KIM, and Byungmin KIM
- 1323 A Generation Method of Amplitude-Only Images with Low Intensity Ranges
..... Wannida SAE-TANG, Masaaki FUJIYOSHI, and Hitoshi KIYA
- 1331 Computing-Based Performance Analysis of Approximation Algorithms for the Minimum Weight Vertex Cover Problem of Graphs Satoshi TAOKA, Daisuke TAKAFUJI, and Toshimasa WATANABE
- 1340 Novel THP Scheme with Minimum Noise Enhancement for Multi-User MIMO Systems
..... Shogo FUJITA, Leonardo LANANTE Jr., Yuhei NAGAO, Masayuki KUROSAKI, and Hiroshi OCHI
- 1348 An Effective Overlap Removable Objective for Analytical Placement
..... Syota KUWABARA, Yukihide KOHIRA, and Yasuhiro TAKASHIMA
- 1357 Concurrent Detection and Recognition of Individual Object Based on Colour and p-SIFT Features
..... Jienan ZHANG, Shouyi YIN, Peng OUYANG, Leibo LIU, and Shaojun WEI
- 1366 A Dual-Mode Deblocking Filter Design for HEVC and H.264/AVC
..... Muchen LI, Jinjia ZHOU, Dajiang ZHOU, Xiao PENG, and Satoshi GOTO
- 1376 Low Complexity Keypoint Extraction Based on SIFT Descriptor and Its Hardware Implementation for Full-HD 60 fps Video Takahiro SUZUKI and Takeshi IKENAGA

- 1384 Parameterization of All Stabilizing Two-Degrees-of-Freedom Simple Repetitive Controllers with Specified Frequency Characteristics Tatsuya SAKANUSHI, Jie HU, and Kou YAMADA
- 1393 Parallelization of Computing-Intensive Tasks of SIFT Algorithm on a Reconfigurable Architecture System Peng OUYANG, Shouyi YIN, Hui GAO, Leibo LIU, and Shaojun WEI
- 1403 A Low Power Tone Recognition for Automatic Tonal Speech Recognizer Jirabhorn CHAIWONGSAI, Werapon CHIRACHARIT, Kosin CHAMNONGTHAI, Yoshikazu MIYANAGA, and Kohji HIGUCHI

**Regular Section
PAPERS**

■ **Digital Signal Processing**

- 1412 Recovery of Missing Samples from Oversampled Bandpass Signals and Its Stability Sinuk KANG, Kil Hyun KWON, and Dae Gwan LEE

■ **Analog Signal Processing**

- 1421 High Precision Analog Data Acquisition System with Signal Transformer Isolation Technique Yoshihiro AKEBOSHI, Seiichi SAITO, and Hideyuki OHASHI

■ **Systems and Control**

- 1429 Relaxed Stability Condition for T-S Fuzzy Systems Using a New Fuzzy Lyapunov Function Sangsu YEH and Sangchul WON

■ **Cryptography and Information Security**

- 1437 Improved Key Recovery Attack on the BEAN Stream Cipher Hui WANG, Martin HELL, Thomas JOHANSSON, and Martin ÅGREN

■ **Spread Spectrum Technologies and Applications**

- 1445 Lower Bounds on the Aperiodic Hamming Correlations of Frequency Hopping Sequences Xing LIU, Daiyuan PENG, Xianhua NIU, and Fang LIU

■ **Intelligent Transport System**

- 1451 Object Detection Using RSSI with Road Surface Reflection Model for Intersection Safety Shoma HISAKA and Shunsuke KAMIJO

■ **Image**

- 1460 A Modified Pulse Coupled Neural Network with Anisotropic Synaptic Weight Matrix for Image Edge Detection Zhan SHI and Jinglu HU
- 1468 An Adaptation Method for Morphological Opening Filters with a Smoothness Penalty on Structuring Elements Makoto NAKASHIZUKA, Yu ASHIHARA, and Youji IIGUNI

LETTERS

■ **Digital Signal Processing**

- 1478 Adaptive Feedback Cancellation on Improved DCD Algorithms Chao DONG, Li GAO, Ying HONG, and Chengpeng HAO
- 1482 Partial-Update Normalized Sign LMS Algorithm Employing Sparse Updates Seong-Eun KIM, Young-Seok CHOI, Jae-Woo LEE, and Woo-Jin SONG

■ **Systems and Control**

- 1488 Iterative Learning Control with Advanced Output Data Using an Estimation of the Impulse Response Gu-Min JEONG and Sang-Hoon JI

■ **Numerical Analysis and Optimization**

- 1492 An Object Based Cooperative Spectrum Sensing Scheme with Best Relay Meiling LI and Anhong WANG

■ **Coding Theory**

- 1496 MacWilliams Type Identity for M -Spotty Rosenbloom-Tsfasman Weight Enumerator of Linear Codes over Finite Ring Jianzhang CHEN, Wenguang LONG, and Bo FU

■ **Measurement Technology**

- 1501 Geometric Predicted Unscented Kalman Filtering in Rotate Magnetic Ranging Chao ZHANG, Keke PANG, and Yaxin ZHANG



-
- 1505 **ABSTRACTS** (IEICE Trans. Fundamentals (Japanese Edition), Vol. J96-A, No. 6)
1507 **Errata** (Vol. E95-A, No. 6: Tomotaka WADA, Toshihiro HORI, Manato FUJIMOTO, Kouichi MUTSUURA, and Hiromi OKADA)

Original Contributions in English

Copyright © 2013 by The Institute of Electronics, Information and Communication Engineers

The IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences has been selected for coverage in the following ISI (Institute for Scientific Information) products/services.

- Science Citation Index Expanded (included in "Web of Science")
- Current Contents (Edition: Engineering, Computing and Technology)
- ISI Alerting Services
- CompuMath Citation Index*

*CompuMath Citation Index includes bibliographic information from over 600 journals, books, and proceedings on computers and mathematics.

