IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

A PUBLICATION OF THE IEEE SIGNAL PROCESSING SOCIETY

www.signalprocessingsociety.org

JANUARY 2013 VOLUME 8 NUMBER 1 ITIFA6 (ISSN 1556-6013)

PAPERS

Applied Cryptography

White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures .... *Z. Liu, Z. Cao, and D. S. Wong* 76

Biometrics

User Authentication Through Mouse Dynamics .... *C. Shen, Z. Cai, X. Guan, Y. Du, and R. A. Maxion* 16

Latent Fingerprint Matching Using Descriptor-Based Hough Transform .... *A. A. Paulino, J. Feng, and A. K. Jain* 31

An Optimized Wavelength Band Selection for Heavily Pigmented Iris Recognition .... *Y. Gong, D. Zhang, P. Shi, and J. Yan* 64

Recognizing Surgically Altered Face Images Using Multiobjective Evolutionary Algorithm .... *H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa* 89

Face Recognition and Verification Using Photometric Stereo: The Photoface Database and a Comprehensive Evaluation ...... *S. Zafeiriou, G. A. Atkinson, M. F. Hansen, W. A. P. Smith, V. Argyriou, M. Petrou, M. L. Smith, and L. N. Smith* 121

Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication .... *M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song* 136

An Evaluation of Otoacoustic Emissions as a Biometric .... *N. J. Grabham, M. A. Swabey, P. Chambers, M. E. Lutman, N. M. White, J. E. Chad, and S. P. Beeby* 174

Matching Composite Sketches to Face Photos: A Component-Based Approach .... *H. Han, B. F. Klare, K. Bonnen, and A. K. Jain* 191

Component-Based Representation in Automated Face Recognition .... *K. Bonnen, B. F. Klare, and A. K. Jain* 239

(Contents Continued on Page 4)

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (ISSN 1556-6013) is published monthly by the Institute of Electrical and Electronics Engineers, Inc. Responsibility for the contents rests upon the authors and not upon the IEEE, the Society/Council, or its members. **IEEE Corporate Office:** 3 Park Avenue, 17th Floor, New York, NY 10016-5997. **IEEE Operations Center:** 445 Hoes Lane, Piscataway, NJ 08854-4141. **NJ Telephone:** +1 732 981 0060. **Price/Publication Information**: Individual copies: IEEE Members $20.00 (first copy only), nonmembers $288.00 per copy. (Note: Postage and handling charge not included.) Member and nonmember subscription prices available upon request. **Copyright and Reprint Permissions:** Abstracting is permitted with credit to the source. Libraries are permitted to photocopy for private use of patrons, provided the per-copy fee indicated in the code at the bottom of the first page is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For all other copying, reprint, or republication permission, write to Copyrights and Permissions Department, IEEE Publications Administration, 445 Hoes Lane, Piscataway, NJ 08854-4141. Copyright © 2013 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved. Periodicals Postage Paid at New York, NY and at additional mailing offices. **Postmaster:** Send address changes to IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE, 445 Hoes Lane, Piscataway, NJ 08854-4141. GST Registration No. 125634188. CPC Sales Agreement #40013087. Return undeliverable Canada addresses to: Pitney Bowes IMEX, P.O. Box 4332, Stanton Rd., Toronto, ON M5W 3J4, Canada. IEEE prohibits discrimination, harassment and bullying. For more information visit http://www.ieee.org/nondiscrimination. Printed in U.S.A.

(Contents Continued from Page 3)

Communication and Physical-Layer Security

Secrecy Capacity Enhancement With Distributed Precoding in Multirelay Wiretap Systems .... *H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang* 229

Network Security

A Real-Time Design Based on FPGA for Expeditious Error Reconciliation in QKD System .... *K. Cui, J. Wang, H.-F. Zhang, C.-L. Luo, G. Jin, and T.-Y. Chen* 184

Forensics Analysis

Document Clustering for Forensic Analysis: An Approach for Improving Computer Inspection .... *L. F. da Cruz Nassif and E. R. Hruschka* 46

Multimedia Content Hash

Robust Hashing for Image Authentication Using Zernike Moments and Local Features .... *Y. Zhao, S. Wang, X. Zhang, and H. Yao* 55

Network Security

COKE: Crypto-Less Over-the-Air Key Establishment .... *R. Di Pietro and G. Oligeri* 163
Decentralized Hypothesis Testing in Wireless Sensor Networks in the Presence of Misbehaving Nodes .... *E. Soltanmohammadi, M. Orooji, and M. Naraghi-Pour* 205

Security of Large Networked Systems

Internet Traffic Classification by Aggregating Correlated Naive Bayes Predictions .... *J. Zhang, C. Chen, Y. Xiang, W. Zhou, and Y. Xiang* 5
On the Security of End-to-End Measurements Based on Packet-Pair Dispersions .... *G. O. Karame, B. Danev, C. Bannwart, and S. Čapkun* 149

Watermarking and Data Hiding

Heap Graph Based Software Theft Detection .... *P. P. F. Chan, L. C. K. Hui, and S. M. Yiu* 101
Reversible Watermarking Based on Invariant Image Classification and Dynamic Histogram Shifting .... *G. Coatrieux, W. Pan, N. Cuppens-Boulahia, F. Cuppens, and C. Roux* 111
Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography .... *C. Yang, F. Liu, X. Luo, and Y. Zeng* 216

CORRESPONDENCE

Biometrics

On Mixing Fingerprints .... *A. Othman and A. Ross* 260

Communication and Physical-Layer Security

Physical Layer Security of TAS/MRC With Antenna Correlation .... *N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen* 254