IEEE TRANSACTIONS ON

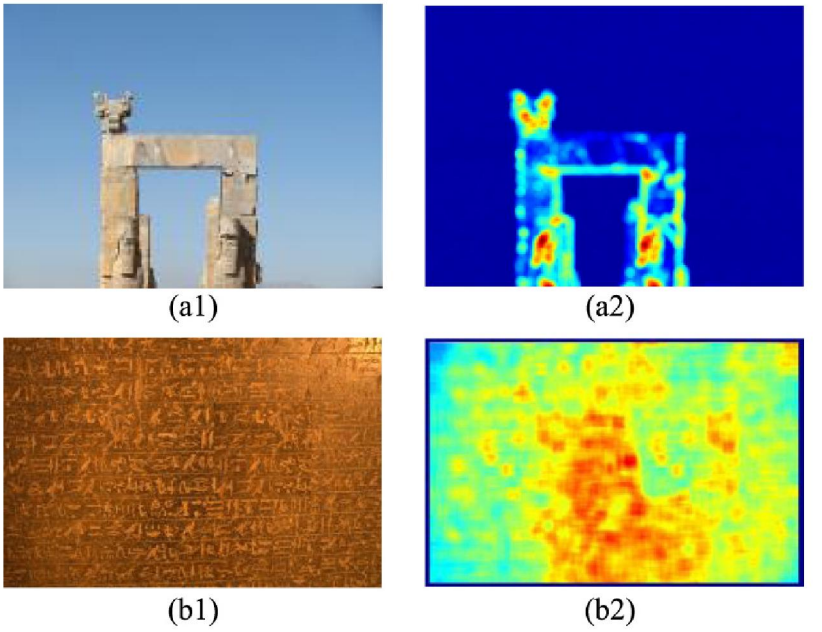
INFORMATION FORENSICS AND SECURITY

A PUBLICATION OF THE IEEE SIGNAL PROCESSING SOCIETY

IEEE Signal Processing Society

www.signalprocessingsociety.org

NOVEMBER 2016	VOLUME 11	NUMBER 11	ITIFA6	(ISSN 1556-6013)
DECEMBER 2016	VOLUME 11	NUMBER 12		



Examples of the uniqueness map: (a1) and (b1) illustrate two forged images; (a2) and (b2) are their corresponding uniqueness map, respectively, as seen in "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector," by M. Zandi *et al.*, p. 2499. Warmer colors indicate more uniqueness.

For the November 2016 issue, see p. 2397 for Table of Contents.
For the December 2016 issue, see p. 2631 for Table of Contents.

IEEE

IEEE TRANSACTIONS ON

INFORMATION FORENSICS AND SECURITY

A PUBLICATION OF THE IEEE SIGNAL PROCESSING SOCIETY

IEEE Signal Processing Society

www.signalprocessingsociety.org

NOVEMBER 2016 VOLUME 11 NUMBER 11 ITIFA6 (ISSN 1556-6013)

REGULAR PAPERS

An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys ..... *X. Liu, R. H. Deng, K.-K. R. Choo, and J. Weng* 2401

DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System ..... *B. Li, R. Lu, W. Wang, and K.-K. R. Choo* 2415

DW-AES: A Domain-Wall Nanowire-Based AES for High Throughput and Energy-Efficient Data Encryption in Non-Volatile Memory ..... *Y. Wang, L. Ni, C.-H. Chang, and H. Yu* 2426

On the Secrecy Capacity of Wiretap Channels With Side Information at the Transmitter ..... *H. Fujita* 2441

Scaling Up Class-Specific Kernel Discriminant Analysis for Large-Scale Face Verification ..... *A. Iosifidis and M. Gabbouj* 2453

Relay Selection for Secure Successive AF Relaying Networks With Untrusted Nodes ..... *W. Wang, K. C. Teh, and K. H. Li* 2466

Efficient Deniably Authenticated Encryption and Its Application to E-Mail ..... *F. Li, D. Zhong, and T. Takagi* 2477

CDMA System Design and Capacity Analysis Under Disguised Jamming ..... *T. Song, K. Zhou, and T. Li* 2487

Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector ..... *M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour* 2499

Privacy-Preserving Outsourced Calculation on Floating Point Numbers ..... *X. Liu, R. H. Deng, W. Ding, R. Lu, and B. Qin* 2513

On Designing Satisfaction-Ratio-Aware Truthful Incentive Mechanisms for k-Anonymity Location Privacy ..... *Y. Zhang, W. Tong, and S. Zhong* 2528

(Contents Continued on Page 2398)

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 $339.00 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 of $31.00 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 © 2016 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved. **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 2397)

2DCrypt: Image Scaling and Cropping in Encrypted Domains ..... *M. Mohanty, M. R. Asghar, and G. Russello* 2542
Secure, Fast, and Energy-Efficient Outsourced Authentication for Smartphones ..... *P. Gasti, J. Šeděnka, Q. Yang, G. Zhou, and K. S. Balagani* 2556
Privacy-Preserving Public Auditing Protocol for Low-Performance End Devices in Cloud ..... *J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong* 2572
A Novel Method Based on Empirical Mode Decomposition for P300-Based Detection of Deception ..... *A. Arasteh, M. H. Moradi, and A. Janghorbani* 2584
A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing ..... *Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren* 2594
Joint Information and Jamming Beamforming for Secrecy Rate Maximization in Cognitive Radio Networks ..... *V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin* 2609

COMMENTS AND CORRECTIONS

Comments on "A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-per-Device Licensing" ..... *L. Bossuet and B. Colombier* 2624
Rebuttal to "Comments on 'A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing'" ..... *J. Zhang and G. Qu* 2626
Corrections to "JPEG Anti-Forensics With Improved Tradeoff Between Forensic Undetectability and Image Quality" ..... *W. Fan, K. Wang, F. Cayre, and Z. Xiong* 2628