Benedetta Tondi

BIRTH DATE May 5, 1987

CITIZENSHIP Italian

SHORT BIOGRAPHY **Benedetta Tondi** received the master degree (*cum laude*) in Electronics and Communications Engineering at the University of Siena in 2012 and her PhD degree in Information Engineering and Mathematical Sciences at the University of Siena in 2016, with a thesis on the Theoretical Foundations of Adversarial Detection and Applications to Multimedia Forensics, in the area of Multimedia Security. She is currently Assistant Professor at the Department of Information Engineering and Mathematics, University of Siena. She has been assistant for the course of Information Theory and Coding, Cybersecurity, Multimedia Security and Mathematical Statistics. She currently teaches the course of Foundations of Telecommunications at the B.S course and Information Theory at the M.S course. She is a member of the Visual Information Processing and Protection (VIPP) Group led by Prof. Mauro Barni. She is part of the IEEE Young Professionals and IEEE Signal Processing Society, and a member of the National Inter-University Consortium for Telecommunications (CNIT). From January 2019, she is also a member of the Information Forensics and Security (IFS) Technical Committee of the IEEE Signal Processing Society. Her research interest focuses on the application to Multimedia Security of Information-Theoretic methods, Game Theory concepts, Optimization Theory methods, and advanced Probability Theory methods, and more in general on the Adversarial Signal Processing. Recently, she is working on Machine Learning and Deep Learning applications for Multimedia Forensics and Counter-Forensics, Fake Media detection, Adversarial Machine Learning, and on the security of Machine Learning techniques.

EDUCATION **University of Siena**, Siena, Italy

PhD degree in Information Engineering and Mathematical Sciences, September 2016

- Adversarial Signal Processing, Information Forensics and Security,
- Thesis Title: *Theoretical Foundations of Adversarial Detection and Applications to Multimedia Forensics*,

M.S. degree in Electronics and Communications Engineering *con lode*, April 2012

- Information Forensics and Security,
- Thesis Title: *Adversary-aware source identification: a game-theoretic approach*,

B.S. degree in Information Engineering *con lode*, October 2009

- Information Forensics and Security,
- Thesis Title: *Analisi forense per l'identificazione della sorgente di un documento stampato*,

Scientific lyceum degree, July 2016.

ACADEMIC CAREER Benedetta Tondi got her PhD degree in Information Engineering and Mathematics at the University of Siena in 2016, working on a theory of Adversarial Signal Processing and Adversarial Detection and on applications to Multimedia Forensics and more in general security-oriented applications.
From October 2014 to February 2015 she has been a visiting student at the University of Vigo at the Signal Processing in Communications Group (GPSC), at the Dept. Teoria de la Senal y Comunicaciones, ETSI Telecom, working on the study of techniques to reveal attacks in watermarking systems. Her stay was funded by a Spanish National Project on Multimedia Security.
From December 2015 to November 2020 she has been Research Fellow at the Department of Information Engineering and Mathematics of the University of Siena. From December 2020 to December 2021 she has been Researcher (RTD-A) at the same Department. In

2018, she was invited visiting researcher at the Israel Institute of Technology, Technion, Haifa.
Currently, she is Assistant Professor (RTD-B) at the Department of Information Engineering and Mathematics of the University of Siena.
She has been assistant for the courses of "Information Theory and Coding" (2015-2016, 2017-2018, 2018-2019, 2019- 2020), "Multimedia Security" (2015-2016, 2016-2017, 2017-2018), "Cybersecurity" (2018/2019-2019/2020) and "Mathematical Statistics" (2020/2021-2021/2022). She co-teaches the course "Fondamenti di Telecomuncazioni" since 2020 (2020/2021-2021/2022- 2022/2023). She teaches the course "Information Theory" since 2022/2023. She is Department Delegate for communication since December 2022.

Research activity and collaborations

Her research interests focus on Multimedia Security, Adversarial Signal Processing, and Multimedia Forensics. Recently, she is working on Deep Learning for Multimedia Forensics and Counter-Forensics, Adversarial Machine Learning and on the Security of Machine Learning techniques.

From 2012, she is participating to the research activity of the research group "Visual Information Processing and Protection Group" (VIPP) led by Prof. Mauro Barni, characterized by several national and international collaborations. In particular, she has been collaborating with the research group led by Yao Zhao e Rongrong Ni, Beijing Jiaotong University, NJTU (China), the group led Mariko Nakano-Miyatake, of the Instituto Politécnico Nacional, Mexico City (IPN), the group led by Stefano Tubaro, Politecnico di Milano, and the group led by Edward Delp, School of Electrical and Computer Engineering Purdue University, within the Medifor an Forensic Analysis of Overhead Images projects; the group led by Xixiang Lv of the Xidian University, Sian (China).

Since 2013 she has been working with Prof. Fernando Pérez-González of the University of Vigo on the study of techniques for securing watermarking systems and on DNN watermarking.

Since 2014 she has been collaborating with the Electrical Engineering Department at the Technion, Israel Institute of Technology of Haifa (Israel), in particular with Prof. Neri Merhav, working on the application of information theory concepts and advanced probability theory methods to multimedia security.

Since 2018, she has been collaborating with Prof. Bin Li of Shenzhen University (China) andhis research group, working on the forensic analysis of JPEG images in adversarial environment by using deep learning techniques.

Projects

Involved in the European REWIND Project, Future and Emerging Technologies (FET) programme within the 7FP of the EC from 2012 to 2014, as participant to the research activity

Task manager (for the UNISI task) of the research project "Media Forensics Integrity Analysis" (MediFor), financed by DARPA and Air Force Research Laboratory, 2016-2020, under agreement number FA8750-16-2-0173.

Task manager of the research project "Research on JPEG image forensics and anti-forensics via deep learning under adversarial conditions" (general program: 2019-2022) founded by the National Natural Science Foundation of China (NSFC), grant number 61872244.

Task manager of the research project "Forensic Analysis of Overhead Images", financed by the National Geospatial-Intelligence Agency (NGA), from 2019

Work Package Coordinator of the research project "PREserving Media trustworthiness in the artificial Intelligence Era" (PREMIER), financed by Italian Ministry - MIUR (Prin project), 2020-2024

Co-Principal Investigator of the research project "DISCOVER: A Data-Driven Integrated Approach for Semantic Inconsistencies Verification", financed by DARPA and Air Force Research Laboratory, 2020-2024, under agreement number FA8750-20-2-1004.

Scientific Responsible of the project "Stealthy Video Backdoor Attacks against DNNs and Defences (BackVid)" founded by the Italian Ministry under the Curiosity-Driven (F-CUR) program (PSR), 2021-2023.

Activity for scientific societies

- Reviewer for the journal IEEE Transactions on Information Forensics and Security, IEEE Signal Processing Letters, IEEE Transactions on Circuits and Systems for Video Technology, IEEE Transactions of Wireless Communications, IEEE Transactions on Dependable and Secure Computing, Elsevier Journal of Visual Communication and Image Representation, IET Information Security, IET Image Processing, MDPI Entropy, Elsevier Computers & Security, Springer Multimedia Tools and Applications.
- Designated reviewer on the Technical Program Committee for the Workshop on Information Forensics and Security (IEEE GlobalSIP-WIFS) 2014, the International Conference on Multimedia and Expo (IEEE ICME) 2016, and the IEEE International Conference on Image Processing (IEEE ICIP) 2015, 2016, 2018 and 2022, and the International Conference on Image Analysis and Processing 2021 and 2022..
- Member of the Technical Program Committee of the International Conference on Multimedia and Expo (IEEE ICME) 2015, the International Carnahan Conference on Security Technologies (ICCST) 2017, the European Signal Processing Conference (EUSIPCO) 2018, the International Conference on Image Analysis, Processing (ICIAP) 2019 and the Workshop on Information Forensics and Security (IEEE WIFS) 2019, the ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC) 2021, the Workshop on Information Forensics and Security (IEEE WIFS) 2021 and International Workshop on Digital-forensics and Watermarking 2022.
- Co-organizer and Chair of the Special Session "Adversarial Multimedia Forensics" at the Eurasip EUSIPCO 2018.
- Elected member of the Information Forensics and Security (IFS) Technical Committee of the IEEE Signal Processing Society (January 1, 2019 - December 31, 2021). Main roles: Area Chair for IFS. Member of the Nominations and Elections Subcommittee.
- Area Chair of IEEE ICASSP 2020 and 2021, IEEE ICIP 2019, 2021 and 2022.
- Session Chair at EUSIPCO 2018, IEEE ICASSP 2019, IEEE WIFS 2019, ACM IH& MMSEC 2021, IEEE ICIP 2021, and IEEE WIFS 2022.
- Co-organizer of the Special Session "Artificial Intelligence for Multimedia Security Applications" at the IEEE ICIP 2019.
- Member of the Organizing Committee of IEEE WIFS 2019 (publication chair).
- Co-organizer and co-chair of the Special Session "DNN Watermarking" at the ACM IH&MMSEC 2021.
- Member of the Organizing Committee of IEEE WIFS 2022 (Area Chair).
- Technical Program Chair at ACM IH&MMSEC 2022.

- Co-organizer of the Special Session " Multimedia Forensics and Security in Deep Learning Era" at the ICIP 2022.
- Invited keynote speaker at ITASEC 2022
- Elected member of the Information Forensics and Security (IFS) Technical Committee of the IEEE Signal Processing Society for the second time (January 1, 2023 - December 31, 2025).
- Member of the Organizing Committee of IEEE WIFS 2023 (Publicity Chair).

EDITORIAL COMMITTEES

Associate Editor of the EURASIP Journal on Information Security (from July 2018 till June 2023).

Guest Editor of the Special Issue on "Dependable Deep Learning for Security-Oriented Applications" in the EURASIP Journal of Information Security.

Guest Editor of the Special Issue on "Information-Theoretic Methods for Deep Learning Based Data Acquisition, Analysis and Security" in the Entropy MDPI journal.

Associate Editor of the IET Information Security (from November 2019 till February 2023).

Review Editor of the Journal Frontiers in Signal Processing, Image Processing (from March 2021).

Associate Editor of Journal Frontiers in Signal Processing, Image Processing (from September 2022).

Guest Editor of the Special Issue on "Robust Deep Learning Techniques for Multimedia Forensics and Security" in the MDPI Journal of Imaging.

Associate Editor of IEEE Information Forensics and Security (from February 2023).

Guest Editor of the Special Issue on "Adversarial Machine Learning: Bridging the Gap between In Vitro and In Vivo Research" at the IEEE Open Journal of Signal Processing.

Associate Editor of IEEE Signal Processing Letters (from June 2023).

MEMBERSHIPS

Member of the National Inter-University Consortium for Telecommunications (CNIT).

Member of the IEEE Signal Processing Society and the IEEE Young Professionals, from 2013.

AWARDS

Best Student Paper Award at the IEEE International Workshop on Information Forensics and Security (WIFS), December 3-5, 2014, Atlanta, Georgia, USA

Best Paper Award at the IEEE International Workshop on Information Forensics and Security (WIFS), November 16-19, 2015, Rome, Italy

Best Paper Award at MMEDIA 2017, The Ninth International Conferences on Advances in Multimedia, April 23-27, 2017, Venezia, Italy

Winner of the 2017 GTTI PhD Award for the best PhD Theses defended at an Italian University in the areas of Communications Technologies (Signal Processing, Digital Communications, Networking).

QUALIFICATION

'Abilitazione scientifica nazionale' received on November 19, 2020 (expiring on November 19, 2029).

Journal Publications

M. Barni, **B. Tondi**."The Source Identification Game: an Information-Theoretic Perspective", *IEEE Transactions on Information Forensics and Security, Vol. 8, no. 3, pp 450-463, March 2013..*

M. Barni, M. Fontani, **B. Tondi**. "A Universal Attack Against Histogram-Based Image Forensics", *International Journal of Digital Crime and Forensics (IJDCF), IGI Global, USA, Vol. 5, no. 3, 2013.*

M. Barni, **B. Tondi**. "Binary Hypothesis Testing Game with Training Data", *IEEE Transactions on Information Theory, Vol. 60, no. 8, pp 4848 - 4866, Aug. 2014.*

A. Abrardo, M. Barni, K. Kallas, **B. Tondi**. "A Game-Theoretic Framework for Optimum Decision Fusion in the Presence of Byzantines", *IEEE Transactions on Information Theory, Vol. 11, no. 6, pp 1333 - 1345, June 2016.*

M. Barni, **B. Tondi**. "Source Distinguishability under Distortion-Limited Attack: an Optimal Transport Perspective", *IEEE Transactions on Information Forensics and Security, Vol. 11, no. 10, pp 2145 - 2159, October 2016.*

B. Tondi, P. Comesana Alfaro, F. Perez-Gonzalez, M. Barni "Smart Detection of Line Search Oracle Attacks", *IEEE Transactions on Information Forensics and Security, Vol. 12, no. 3, pp 588 - 603, March 2017.*

M. Barni, L. Bondi, N. Bonettini, P. Bestagini, A. Costanzo, M. Maggini, **B. Tondi**, S. Tubaro, "Aligned and non-aligned double JPEG detection using convolutional neural networks", *Journal of Visual Communication and Image Representation, Elsevier, Vol. 49, 2017, pp 153-163*

A. Abrardo, M. Barni, K. Kallas, **B. Tondi**. "A Message Passing Approach for Decision Fusion in Adversarial Multi-Sensor Networks", *Information Fusion Journal, Elsevier, Vol. 40, pp 101–111, March 2018.*

M. Barni, **B. Tondi**. "Adversarial Source Identification Game with Corrupted Training", *IEEE Transactions on Information Theory, Vol.64 , No. 5 , May 2018.*

B. Tondi, N. Merhav, M. Barni. "Detection Games Under Fully Active Adversaries", *Entropy 2019, 21, 23.*

M. Barni, H. Santoyo Garcia, **B. Tondi**. "An Improved Statistic for the Pooled Triangle Test against PRNU-Copy Attack", *IEEE Signal Processing Letters, Volume: 25 , Issue: 10 , Oct. 2018 .*

B. Tondi, "Pixel-domain Adversarial Examples Against CNN-based Manipulation Detectors", *Electronics Letters, 2018, Vol. 54, No. 21*

Z. Chen, **B. Tondi**, X. Li, R. Ni, Y. Zhao, M. Barni. "Secure Detection of Image Manipulation by means of Random Feature Selection", *IEEE Transactions on Information Forensics and Security, Vol. 14, Issue. 9, Sept. 2019.*

Y.Niu, **B. Tondi**, Y.Zhao, M.Barni, "Primary Quantization Matrix Estimation of Double Compressed JPEG Images via CNN", *IEEE Signal Processing Letters, Vol. 27, pp 191-195, Dec. 2019.*

M.Barni, E. Nowroozi, **B. Tondi**, "Improving the Security of Image Manipulation Detection through One-and-a-half-class Multiple Classification", *Multimedia Tools and Applications, Springer, Vol. 79, pp 2383–2408, Jan. 2020.*

M.Barni, Q-T.Phan, **B. Tondi**, "Copy Move Source-Target Disambiguation through Multi-Branch CNNs", *IEEE Transactions on Information Forensics and Security, Vol. 16, pp. 1825 - 1840, Dec. 2020..*

W.Guo, **B. Tondi**, M.Barni, "A Master Key Backdoor for Universal Impersonation Attack against DNN-based Face Verification", *Pattern Recognition Letters, Vol. 144, pp. 61-67, 2021.*

B.Zhang, **B. Tondi**, M.Barni, "Adversarial examples for replay attacks against CNN-based face recognition with anti-spoofing capability", *Elsevier Journal on Computer Vision and Image Understanding (CVIU), Vol. 197–198, August 2020.*

B.Zhang, **B. Tondi**, M.Barni, "Challenging the adversarial robustness of DNNs based on error-correcting output codes", *Security and Communication Networks, Vol. 2020, Nov. 2020.*

X.Shi, **B. Tondi**, B.Li, M.Barni, "CNN-based Steganalysis and Parametric Adversarial Embedding: a Game-Theoretic Framework", *Elsevier Journal on Signal Processing: Image Communication, Vol. 89, Nov. 2020.*

B. Tondi, A.Costanzo, D Huang, B.Li, "Boosting CNN-based primary quantization matrix estimation of double JPEG images via a classification-like architecture", *EURASIP Journal on Information Security, Vol. 5, 2021.*

Y.Niu, **B. Tondi**, Y.Zhao, R.Ni, M.Barni, "Image Splicing Detection, Localization and Attribution via JPEG Primary Quantization Matrix Estimation and Clustering", *IEEE Transactions on Information Forensics and Security, Vol.16, Nov. 2021.*

Y Li, **B. Tondi** and M Barni, "Spread-transform dither modulation watermarking of deep neural network", *Elsevier Journal of Information Security and Applications, Vol. 63 2021.*

W Guo, **B. Tondi** and M Barni "A Master Key backdoor for universal impersonation attack against DNN-based face verification", *Pattern Recognition Letters, Vol 144, 61-67, 2021.*

J. Wang, O. Alamayreh, **B. Tondi** , A. Costanzo and M. Barni "Detecting Deepfake Videos in Data Scarcity Conditions by Means of Video Coding Features", *APSIPA Transactions on Signal and Information Processing, Vol 11, 2022.*

L. Abady, J. Horvath, **B. Tondi**, E. J Delp and M. Barni, "Manipulation and Generation of Synthetic Satellite Images Using Deep Learning Models" , *Journal of Applied Remote Sensing (JARS), Vol 16, 2022.*

Guo, Wei, **B. Tondi**, and Mauro Barni. "An overview of backdoor attacks against deep neural networks and possible defences" *IEEE Open Journal of Signal Processing, Vol 3, 2022.*

L.Abady, E.D. Cannas, P.Bestagini, **B. Tondi**, S.Tubaro and M.Barni, "An Overview on the Generation and Detection of Synthetic and Manipulated Satellite Images", *APSIPA Transactions on Signal and Information Processing, Vol 11, 2022.*

W Guo, **B. Tondi**, M Barni, "A temporal chrominance trigger for clean-label backdoor attack against anti-spoof rebroadcast detection" *IEEE Transactions on Dependable and Secure Computing (2023).*

O. Alamayreh, C. Fascella, S. Mandelli, **B. Tondi**, P. Bestagini, and M. Barni, "Just Dance: Detection of human body reenactment fake videos", *(submitted to EURASIP Journal on Image and Video Processing, 2022)*

W.Guo, **B. Tondi** and M.Barni, "Universal Detection of Backdoor Attacks via Density-based Clustering and Centroids Analysis", *submitted to IEEE TIFS*

Conference Publications

M. Barni, M. Fontani, **B. Tondi**. "A Universal Technique to Hide Traces of Histogram-Based Image Manipulations". *In proc. of the 14th ACM workshop on Multimedia and Security*, MMSEC 2012.

M. Barni, **B. Tondi**. "Optimum Forensic and Counter-forensic Strategies for Source Identification with Training Data". *In Proc. of IEEE International Workshop on Information Forensics and Security*, WIFS 2012.

M. Barni, **B. Tondi**. "Multiple-Observation Hypothesis Testing under Adversarial Conditions". *Proc. of WIFS'13, IEEE International Workshop on Information Forensics and Security, 18-21 November 2013, Guangzhou, China*,

M. Barni, **B. Tondi**. "The Security Margin: a Measure of Source Distinguishability under Adversarial Conditions". *Proc. of GlobalSip'13, IEEE Global Conference on Signal and Information Processing, 3-5 December 2013, Austin, Texas*,

F. Perez-Gonzalez, P. Comesana Alfaro, M. Barni, **B. Tondi**. "Are you threatening me?: Towards smart detectors in watermarking". *IS&T/SPIE Electronic Imaging 2014, 2-6 February 2014, San Francisco, California, United States*,

M. Barni, **B. Tondi**. "Source Distinguishability under corrupted training". *Proc. of WIFS'14, IEEE International Workshop on Information Forensics and Security, 3-5 December 2014, Atlanta, Georgia*,

M. Barni, **B. Tondi**. "Universal Counterforensics of Multiple Compressed JPEG Images". *IWDW 2014, The 13th International Workshop on Digital-forensics and Watermarking, October 01-04, 2014, Taipei, Taiwan*

A. Abrardo, M. Barni, K. Kallas, **B. Tondi**. "Decision fusion with corrupted reports in multi-sensor networks: A game-theoretic approach" *Proc.of CDC 2014, IEEE 53rd Annual Conference on Decision and Control (CDC), 15-17 Dec. 2014, Los Angeles, CA*

B. Tondi, P. Comesana Alfaro, F. Perez-Gonzalez, M. Barni. "The Effectiveness of the Meta-Detection for Countering Oracle Attacks in Watermarking" *WIFS'15, IEEE International Workshop on Information Forensics and Security (WIFS), 16-19 Nov. 2015, Rome, Italy*

B. Tondi, M. Barni, N. Merhav. "Detection Games with a Fully Active Attacker" *WIFS'15, IEEE International Workshop on Information Forensics and Security (WIFS), 16-19 Nov. 2015, Rome, Italy*

M. Barni, Z. Chen, **B. Tondi**. "Adversary-aware, data-driven detection of double JPEG compression: how to make counter-forensics harder", *WIFS'16, IEEE International Workshop on Information Forensics and Security (WIFS), 4-7 December, 2016, Abu Dhabi, UAE*

K. Kallas, **B. Tondi**, R.Lazzeretti, M. Barni. "Consensus Algorithm with Censored Data for Distributed Detection with Corrupted Measurements: A Game-Theoretic Approach", *2016 Conference on Decision and Game Theory for Security (GameSec), 2-4 November, 2016, New York, USA*

M. Barni, **B. Tondi**. "Threat Models and Games for Adversarial Multimedia Forensics" *MFSec17, Proceedings of the 2nd International Workshop on Multimedia Forensics and Security, 6-10 June, 2017, Bucharest, Romania*

A. Abrardo, M. Barni, K. Kallas, **B. Tondi**. "A Message Passing Approach for Decision Fusion of Hidden-Markov observations in the presence of Synchronized Attacks in Sensor Networks" *MMEDIA 2017 : The Ninth International Conferences on Advances in Multimedia , 23-27 April, 2017, Venezia, Italy*

M. Barni, E. Nowroozi, **B. Tondi**. "Higher-order, adversary-aware, double jpeg-detection via selected training on attacked samples", *EUSIPCO17, European Signal Processing Conference, 28 August- 2 September, 2017, Kos Island, Greece*

Z. Chen, **B. Tondi**, X. Li, R. Ni, Y. Zhao, M. Barni. "A gradient-based pixel-domain attack against SVM detection of global image manipulations ", *WIFS'17, 4-7 December, 2017, Rennes, France*

A. Abrardo, M. Barni, K. Kallas, **B. Tondi**. "Decision Fusion with Unbalanced Priors under Synchronized Byzantine Attacks: a Message-Passing Approach," Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Honolulu, Hawaii, November 2018.

M. Barni, E. Nowroozi, **B. Tondi**. "Detection of adaptive histogram equalization robust against JPEG compression", *6th IAPR/IEEE International Workshop on Biometrics and Forensics (IWBF), June 7, 8 2018, Sassari, Italy.*

M. Barni, A. Costanzo, E. Nowroozi, **B. Tondi**. "CNN-based detection of generic contrast adjustment with JPEG post-processing" *IEEE International Conference on Image Processing (ICIP) October 7-10, 2018, Athens, Greece.*

M. Barni, M. C. Stamm, **B. Tondi**. "Adversarial Multimedia Forensics: Overview and Challenges Ahead", *E*uropean Signal Processing Conference (EUSIPCO), Rome, Italy, September 2018.

M. Barni, Mariko Nakano-Miyatake, H. Santoyo Garcia, **B. Tondi**. "Countering the Pooled Triangle Test for PRNU-based camera identification". *IEEE International Workshop on Information Forensics and Security (WIFS), December 11-13, 2018, Honk Kong.*

M. Barni, E. Nowroozi, K Kallas, **B. Tondi**. "On the transferability of adversarial examples against CNN-based image forensics", *International Conference on Acoustics, Speech, and Signal Processing ICASSP, May 11-17, 2019, Brighton, UK.*

M. Barni, K Kallas, **B. Tondi**, "A new Backdoor Attack in CNNs by training set corruption without label poisoning", *IEEE International Conference on Image Processing (ICIP 2019), Taipei, Taiwan, September 22-25, 2019.*

A Bhalerao, K Kallas, **B. Tondi**, M. Barni. "Luminance-based video backdoor attack against anti-spoofing rebroadcast detection", *IEEE 21st International Workshop on Multimedia Signal Processing (MMSP 2019), Kuala Lumpur, Malaysia, September 27-29, 2019.*

M. Barni, D Huang, B.Li, **B. Tondi**, "Adversarial CNN Training Under JPEG Laundering Attacks: a Game-Theoretic Approach", *IEEE International Workshop on Information Forensics and Security (WIFS), December 9-12, 2019, Delft, Netherland.*

M. Barni, E Nowroozi, **B. Tondi**, B Zhang, "Effectiveness of random deep feature selection for securing image manipulation detectors against adversarial examples", *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), May 5-9, 2020, Barcelona, Spain.*

L. Abady, M. Barni, A. Garzelli, **B. Tondi**, "GAN Generation of Synthetic Multispectral Satellite Images", *SPIE remote sensing, September 21-24, 2020, Edinburgh, United Kingdom.*

M. Barni, K.Kallas, E.Nowroozi, **B. Tondi**, "CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Analysis", *IEEE International Workshop on Information Forensics and Security (WIFS), December 6-11, 2020, New York, USA.*

W. Li, **B. Tondi**, R.Ni, M. Barni,"Increased-confidence adversarial examples for improved transferability of counter-forensic attacks." *International Conference on Pattern Recognition (ICPR), January 10-15, 2020, Milan, Italy.*

M. Barni, F. Perez-Gonzalez, **B. Tondi**, "DNN Watermarking: Four Challenges and a Funeral" *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC), June 22-25, 2021, Brussels, Belgium.*

W.Guo, **B. Tondi**, M. Barni, "MasterFace Watermarking for IPR Protection of Siamese Network for Face Verification" *Digital Forensics and Watermarking (IWDW) 2021.*

J. Wang, O. Alamayreh, **B. Tondi** and M. Barni, "An Architecture for the detection of GAN-generated Flood Images with Localization Capabilities", *IEEE 14th Image, Video, and Multidimensional Signal Processing Workshop (IVMSP), 2022.*

D. Li, **B. Tondi**, B. Li, M. Barni "Exploiting temporal information to prevent the transferability of adversarial examples against deep fake detectors", *Proc. of International Joint Conference on Biometrics (IJCB), Abu Dhabi, 10-13 October 2022*

J. Fei, Z. Xia, **B. Tondi** and M. Barni "Supervised GAN Watermarking for Intellectual Property Protection", *IEEE International Workshop on Information Forensics and Security (WIFS) 2022*

O. Alamayreh, G.M. Dimitri, J. Wang, **B. Tondi** and M. Barni, " Which country is this picture from? New data and methods for DNN-based country recognition", *accepted for publication at ICASSP 2023.*

J. Wang, **B. Tondi** and M. Barni, "Classification of synthetic facial attributes by measn of hybrid classification/localization patch-based analysis", *accepted for publication at ICASSP 2023.*

Books

M. Barni, **B. Tondi**, "Theoretical Foundation of Adversarial Binary Detection" *NOW Foundations and Trends in Communications and Information Theory*, 2020.

A. Abrardo, M. Barni, K. Kallas, **B. Tondi**, "Information Fusion in Distributed Sensor Networks with Byzantines" *Springer Signals and Communication Technology*, 2020.

Book chapters

M. Barni, W.Li, **B. Tondi**, B.Zhang "Adversarial Examples in Image Forensics" in Multimedia Forensics, *Springer Nature*