WIFS 2015

7th IEEE International Workshop on Information Forensics and Security

November 16-19, 2015, Rome, Italy

Final Program and Abstract Book

Table of Contents

Welcome from the General Chairs

Omnes viae Romam ducunt

It is our great pleasure to welcome you to the 7th IEEE Workshop on Information Forensics and Security, WIFS 2015. WIFS is the annual flagship workshop of the Information Forensics and Security (IFS) Technical Committee of the IEEE Signal Processing Society. Its major goal is to bring together researchers in the field, to foster ideas exchange and to allow cross-fertilization among researchers working in the different areas of information security. Since its inception in 2009, WIFS has become a prominent forum for cutting-edge research in areas of multimedia forensic analysis, biometrics, data hiding, and more in general topics in the overlap of information security and multimedia signal processing.

This year, the workshop is hosted by Roma Tre University in Rome, Italy, organized by the Section of Applied Electronics at the Department of Engineering.

The workshop will feature instructive tutorials, inspiring plenary talks, and a very high level technical program including both oral and poster sessions, on-going work presentations, demos, and presentations of selected papers published on IEEE Transactions on Information Forensic and Security and on IEEE Signal Processing Letters. The technical program will be complemented by an exciting social program that will allow the attendees to be inspired by the unforgettable beauties of the Haeternal City and to enjoy the renowned Italian cuisine during the gala dinner in one of the most beautiful roof garden in the World.

We would like to thank the IEEE Signal Processing Society, the IEEE Biometric Council, the IFS-TC, and EURASIP for the Workshop technical sponsorship and the IEEE Signal Processing Society for having provided a number of travel grants for attending the Workshop.

In addition, we would like to thank the technical program chairs, Fernando Perez-Gonzalez and Slava Voloshynovskiy for having assembled such interesting program, and the reviewers, both for the inestimable value of their reviews and for helping the program chairs meet stiff deadlines.

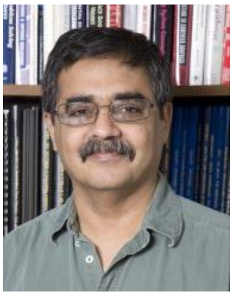
Moreover, we would also like to thank Roma Tre University for hosting the workshop and our sponsors Telecom Italia – TIM, Green Bit, Technicolor, and Mitsubushi Electric for their support.

We would finally like to express our appreciation to all the authors and attendees.

We hope that you will find this workshop a valuable source of thought-provoking results and opportunities to discuss emerging ideas with leading researchers from around the world.

The WIFS 2015 General Chairs
Patrizio Campisi and Nasir Memon

Patrizio Campisi received the Ph.D. degree in electrical engineering from Roma Tre University, Rome, Italy, where he is currently a Full Professor with the Section of Applied Electronics, Department of Engineering. Specifically, he has been working on secure biometric recognition, digital watermarking, image deconvolution, image analysis, stereo image and video processing, blind equalization of data signals, and secure communications. His research interests are in the area of secure multimedia communications and biometrics. He is a co-recipient of the IEEE ICIP06 and the IEEE BTAS 2008 Best Student Paper Award and the IEEE Biometric Symposium 2007 Best Paper Award. He is the General Chair of the seventh IEEE Workshop on Information Forensics and Security (WIFS) 2015, Rome, Italy. He was the General Chair of the 12th ACM Workshop on Multimedia and Security, Rome, in 2010, and General co-Chair of IEEE BIOMS, Rome, in 2014. He is the Editor of the book Security and Privacy in Biometrics (Springer, 2013). He is a Coeditor of the book Blind Image Deconvolution: Theory and Applications (CRC press, 2007). He has been an Associate Editor of the IEEE Signal Processing Letters and the IEEE Transactions On Information Forensics And Security. He is currently a Senior Associate Editor of the IEEE Signal Processing Letters. He is the IEEE SPS Director Student Services. He is a member of the IEEE Technical Committee on Information Assurance and Intelligent Multimedia–Mobile Communications, System, Man, and Cybernetics Society and was a member of the IEEE Certified Biometric Program Learning System Committee.



Nasir Memon is a professor in the Department of Computer Science and Engineering at NYU Polytechnic School of Engineering and the founder and director of the Information Systems and Internet Security (ISIS) laboratory (isis.poly.edu). He is the founding director of the Center for Interdisciplinary Studies in Security and Privacy (CRISSP http://engineering.nyu.edu/crissp/) , and CRISSP Abu Dhabi (http://nyuad.nyu.edu/en/research/nyuad-institute/institute-research/cris...) a collaborative initiative of multiple schools within NYU including NYU-Steinhardt, NYU-Wagner, NYU-Stern, and NYU-Courantas well as NYU Abu Dhabi.

He is an affiliate faculty at the computer science department in the Courant Institute of Mathematical Sciences at NYU. His research interests include digital forensics, biometrics, data compression, network security and security and human behavior. Memon earned a BE in Chemical Engineering and a MS in Mathematics from BITS Pilani, India. He received a MS and PhD in Computer Science from the University of Nebraska. He has published over 250 articles in journals and conference proceedings and holds a dozen patents in image compression and security. He has won several awards including the Jacobs Excellence in Education award and several best paper awards. He has been on the editorial boards of several journals and was the Editor-In-Chief of the IEEE Transactions on Information Security and Forensics. He is an IEEE Fellow and an SPIE Fellow for his contributions to image compression and multimedia security and forensics. Memon was the co-founder of Digital Assembly and Vivic Networks, two early-stage start-ups in NYU-Poly's business incubators.

Welcome from the Technical Program Chairs

It is our pleasure to welcome you to the 2015 IEEE Workshop on Information Forensics and Security (WIFS 2015) sponsored by the IEEE Signal Processing Society. WIFS is the primary annual event organized by the IEEE Information Forensics and Security Technical Committee and has become the foremost meeting place for researchers, engineers and scientists for exchanging ideas and fostering collaborations in this field. WIFS 2015 received 151 submissions of which 55 were accepted, thus reflecting the selective standards of this workshop. The quality of the submissions was extremely high, and so the technical committee worked very hard to compile a program consisting of outstanding papers, with most of them receiving four independent reviews and a minimum of three.

We hope and trust that you will find the WIFS 2015 technical program of interest and excitement including the tutorials and keynote talks by Rainer Böhme, Jean-Pierre Hubaux and Boris Škorić. The workshop will also host a special session on physical layer security organized by Rafael F. Schaefer and H. Vincent Poor who have managed to bring in five outstanding presentations. Besides the ongoing work and poster sessions, now traditional at WIFS, the workshop will feature two novelties that will enhance its liveliness: a collection of nine posters presenting papers recently published in IEEE TIFS/SPL journals, and parallel sessions. Finally, the technical program also includes a felicitous thematic meeting organized by Drs. Barni, Piva and De Rosa, that explores the social and legal implications of multimedia forensics.

We are grateful to the General Chairs, Patrizio Campisi and Nasir Memon, for keeping us on track and last, but not least, the WIFS 2015 Program Committee and the external reviewers whose disinterested help makes it all possible.

The WIFS 2015 Technical Program Chairs
Fernando Pérez-Gonzalez and Slava Voloshynovskiy

Fernando Pérez-González received the Ph.D. in Telecommunications Engineering in 1993. He is currently Full Professor at the University of Vigo, Spain, and Research Professor at the University of New Mexico. His research interests lie in the crossroads of signal processing, security/privacy and communications, in particular, those problems in which an adversary is present. Fernando has coauthored more than 200 journal and conference papers, 15 patents, and has participated in 5 European projects related to multimedia security. He has served in the Editorial Board of several international journals, including IEEE Trans. on Information Forensics and Security. He has been in the program committee of more than 100 conferences and workshops.

Slava Voloshynovskiy received a radio engineer degree from Lviv Polytechnic Institute, Lviv, Ukraine, in 1993 and a Ph.D. degree in electrical engineering from the State University Lvivska Polytechnika, Lviv, Ukraine, in 1996. From 1998 to 1999, he was a visiting scholar with the University of Illinois at Urbana-Champaign. Since 1999, he has been with the University of Geneva, Switzerland, where he is currently an Associate Professor with the Department of Computer Science and head of the Stochastic Information Processing group. His current research interests are in information-theoretic aspects of digital data hiding, content fingerprinting, physical object security, stochastic image modeling and machine learning. He has coauthored over 200 journal and conference papers in these areas and holds ten patents. He served as Associate Editor for IEEE Transactions on Information Forensics and Security (2013-2015). S. Voloshynovskiy was an elected member of the IEEE Information Forensics and Security Technical Committee (2011-2013) where he was area chair in information-theoretic security and an associated member since 2015. He was a general chair of ACM Multimedia Security Conference, 2006 and technical co-chair of Workshop on Information Forensics and Security WIFS15, 2015. He has served as a consultant to private industry in the above areas. He was a recipient of the Swiss National Science Foundation Professorship Grant in 2003.

Program at a Glance

Monday, 16 November 2015

10:00-12:30: **Half-Day Tutorials**

12:30-14:00: **Lunch**

14:00-16:30: **Half-Day Tutorials**

14:00-18:30: **Thematic Meeting**

19:30-21:00: **Welcome Reception**

Tuesday, 17 November 2015

9:00- 9:20: **Welcome** (Aula Magna)

9:20-10:40: **Oral session: Biometrics I** (Aula Magna)

9:20-10:40: **Oral Session: Steganography and Steganalysis** (Aula del Consiglio)

10:40-11:10: **Communication Break**

11:10-12:30: **Oral Session: Robust Hashing** (Aula Magna)

12:30-14:00: **Lunch**

12:30-14:00: **Technical Meeting: IEEE TIFS Editorial Board**

14:00-15:00: **Keynote Talk** (Aula Magna)

15:00-16:40: **Oral Session: Device Security** (Aula Magna)

16:40-17:10: **Communication Break**

17:10-18:30: **Poster Session** (Foyer)

17:10-18:30: **Demo/Ongoing Session** (Foyer)

17:10-18:30: **TIFS/SPL Papers Session** (Foyer)

18:30-21:00: **IEEE Signal Processing Society Chapter Meeting**

Wednesday, 18 November 2015

9:00-10:40: Special Session: Physical Layer Security (Aula Magna)

10:40-11:10: Communication Break

11:10-12:30: Oral Session: Multimedia Forensics I (Aula Magna)

11:10-12:30: Oral Session: Biometrics II (Aula del Consiglio)

12:30-14:00: Lunch

12:30-14:00: Technical Meeting: Information Forensics and Security Technical Committee

14:00-15:00: Keynote Talk (Aula Magna)

15:00-20:00: Social Event

20:00: Gala Dinner

Thursday, 19 November 2015

9:00-10:40: Oral Session: Watermarking and Data Hiding (Aula Magna)

10:40-11:10: Communication Break

11:10-12:30: Oral Session: Adversarial Detection (Aula Magna)

12:30-14:00: Lunch

14:00-15:00: Keynote Talk (Aula Magna)

15:00-16:40: Oral Session: Network Security And Privacy (Aula Magna)

16:40-17:10: Communication Break

17:10-18:30: Oral Session: Multimedia Forensics II (Aula Magna)

	Monday November 16, 2015		Tuesday November 17, 2015		Wednesday November 18, 2015		Thursday November 19, 2015
7:30 - 8:00			Registration				
8:00 - 9:00					Registration		Registration
9:00 - 9:20	Registration		**Welcome**		**Special Session: Physical Layer Security**		**Watermarking and Data Hiding**
9:20 - 10:00			**Biometrics I**	**Steganography and Steganalysis**			
10:00 - 10:40	**Half-day Tutorials**: • Privacy-Aware Data Analytics • Adversarial Signal Processing						
10:40 - 11:10			Communication Break		Communication Break		Communication Break
11:10 - 12:30			**Robust Hashing**		**Multimedia Forensics I**	**Biometrics II**	**Adversarial Detection**
12:30 - 14:00	Lunch		Lunch	**Technical Meeting:** IEEE TIFS Editorial Board	Lunch	**Technical Meeting** IFS – TC	Lunch
14:00 - 15:00	**Half-day Tutorials**: • Privacy in Smart Metering Systems • The Open Set Recognition Problem in Information Forensics and Security	**Thematic Meeting:** Multimedia Truthfulness Verification in Legal Environment and Social Media	**Keynote Talk**: Smoking Blocks - Fighting and Preventing Crime with Virtual Currencies		**Keynote Talk**: Privacy and Security in the Genomic Era		**Keynote Talk**: Dealing with noisy data in biometrics and PUFs
15:00 - 16:40			**Device Security**		**Social Event**		**Network Security and Privacy**
16:40 - 17:10			Communication Break				Communication Break
17:10 - 18:30			**Poster, Demo/Ongoing and TIFS/SPL Papers Sessions**				**Multimedia Forensics II**
18:30 - 19:00			**IEEE Signal Processing Society Chapter Meeting**				
19:00 - 20:00	**Welcome Reception**						
Evening					**Gala Dinner**		

WIFS 2015 Organizing Committee

General Chair

- Patrizio Campisi, *Roma Tre University, Rome, Italy*

General co-Chair

- Nasir Memon, *New York University, New York, USA*

Technical Program Chairs

- Fernando Pérez-González, *University of Vigo, Vigo, Spain*
- Slava Voloshynovskiy, *University of Geneva, Geneva, Switzerland*

Tutorials Chairs

- Tanya Ignatenko, *Eindhoven University of Technology, Eindhoven, Netherlands*
- Zekeriya Erkin, *Delft University of Technology, Delft, Netherlands*

Demo Session Chair

- Samson Cheung, *University of Kentucky, Lexington, Kentucky, USA*

Publications Chair

- Emanuele Maiorana, *Roma Tre University, Rome, Italy*

Finance Chair

- Stefano Tubaro, *Polytechnic University of Milan, Milan, Italy*

Publicity Chairs

- Marco Carli, *Roma Tre University, Rome, Italy*
- Anderson Rocha, *University of Campinas, Barão Geraldo, Campinas, Brasil*

Industry Liaison

- Dinei Florencio, *Microsoft Research, USA*
- Hervé Chabanne, *Morpho, France*
- Tomas Filler, *Digimarc, USA*

European Liaison

- Jana Dittman, *University of Magdeburg, Magdeburg, Germany*

American Liaison

- Arun Ross, *Michigan State University, USA*

Asian Liaison

- Alex C. Kot, *Nanyang Technological University, Singapore*

Local Arrangements Chair

- Federica Battisti, *Roma Tre University, Rome, Italy*

WIFS 2015 TPC Members

- Don Adjeroh, *West Virginia University, USA*
- Mauro Barni, *University of Siena, Italy*
- Patrick Bas, *Ecole Centrale de Lille, France*
- Magdy Bayoumi, *University of Louisiana, USA*
- Vijayakumar Bhagavatula, *Carnegie Mellon University, USA*
- Tiziano Bianchi, *Polytechnic University of Turin, Italy*
- Giulia Boato, *University of Trento, Italy*
- Rainer Bohme, *University of Munster, Germany*
- Terrance Boult, *Univeristy of Colorado, USA*
- Christoph Busch, *Fraunhofer Institute, Germany*
- Patrizio Campisi, *Roma Tre University, Italy*
- Francois Cayre, *Grenoble INP, France*
- Herve Chabanne, *Morpho, France*
- Marc Chaumont, *LIRMM, France*
- Charles Clancy, *Virginia Tech, USA*
- Pedro Comesana-Alfaro, *University of Vigo, Spain*
- Jana Dittmann, *Otto-von-GuerickeUniversität Magdeburg, Germany*
- Gwenaël Doërr, *Technicolor, France*
- Ann Dooms, *Vrije Universiteit Brussel, Belgium*
- Jean-Luc Dugelay, *Eurecom, France*
- Paul Duplys, *Robert Bosch GmbH, Germany*
- Zekeriya Erkin, *Delft University of Technology, Netherlands*
- Farzad Farhadzadeh, *Technical University of Eindhoven, Netherlands*
- Tomas Filler, *Digimarc, USA*
- Dinei Florencio, *Microsoft Research, USA*
- Patrick Flynn, *University of Notre Dame, USA*
- Caroline Fontaine, *Telecom-Bretagne, France*
- Jessica Fridrich, *SUNY, Binghamton, USA*
- Teddy Furon, *INRIA - Rennes - Bretagne Atlantique, France*
- Miroslav Goljan, *State University of New York, USA*
- Anthony T.S. Ho, *University of Surrey, UK*
- Y.-W. Peter Hong, *National Tsing Hua University, Taiwan*
- Chiou-Ting Candy Hsu, *National Tsing Hua University, Taiwan*
- Jiwu Huang, *Shenzhen University, China*
- Tanya Ignatenko, *Eindhoven University of Technology, Netherland*
- Xudong Jiang, *Nanyang Technological University, Singapore*
- Ton Kalker, *DTS, Inc., USA*
- Ramesh Karri, *Polytechnic Institute of NYU, USA*
- Stefan Katzenbeisser, *TU Darmstadt, Germany*
- Matthias Kirchner, *State University of New York , USA*
- Hitoshi Kiya, *Tokyo Metropolitan University, Japan*
- Negar Kiyavash, *University of Illinois at Urbana-Champaign, USA*
- Alex Kot, *Nanyang Technical University, Singapore*

- C.-C. Jay Kuo, *University of Southern California, USA*
- Inald Lagendijk, *Delft University of Technology, Netherlands*
- Jiangtao Li, *Google, USA*
- Mark Liao, *Institute of Information Science, Academia Sinica, Taiwan*
- Emanuele Maiorana, *Roma Tre University, Italy*
- Sebastien Marcel, *IDIAP Research Institute, Switzerland*
- Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
- Nasir Memon, *New York University, USA*
- Pierre Moulin, *University of Illinois at Urbana-Champaign, USA*
- Corina Nafornita, *"Politehnica" University of Timisoara, Romania*
- Karthik Nandakumar, *IBM, USA*
- Sharath Pankanti, *IBM, USA*
- Luis Perez-Freire, *Gradiant, Spain*
- Fernando Perez-Gonzalez, *University of Vigo, Spain*
- Tomas Pevny, *Czech Technical University in Prague, Czech Republic*
- Alessandro Piva, *University of Florence, Italy*
- H. Vincent Poor, *Princeton University, USA*
- Bart Preneel, *Katholieke Universiteit Leuven, Belgium*
- Shantanu Rane, *Palo Alto Research Center (PARC), USA*
- Anderson Rocha, *University of Campinas, Brazil*
- Arun Ross, *Michigan State University, USA*
- Enriquearagones Rua, *Gradiant, Spain*
- Wadih Sawaya, *Telecom-Lille, France*
- Rafael Schaefer, *Princeton University, USA*
- Walter Scheirer, *Harvard University, USA*
- Husrev T. Sencar, *TOBB University, Turkey*
- Samson Sen-Sing Cheung, *University of Kentucky, USA*
- Yun Q. Shi, *New Jersey Institute of Technology, USA*
- Boris Skoric, *Technische Universiteit Eindhoven, Netherlands*
- Matthew Stamm, *Drexel University, USA*
- Yan Lindsay Sun, *University of Rhode Island, USA*
- Marco Tagliasacchi, *Polytechnic University of Milan, Italy*
- Benjamin Tams, *University of Goettingen, Germany*
- Andrew Teoh, *Yonsei University, South Korea*
- Wade Trappe, *WINLAB, Rutgers University, USA*
- Juan Ramón Troncoso Pastoriza, *University of Vigo, Spain*
- Andreas Uhl, *Salzburg University, Austria*
- Avinash Varna, *Intel, USA*
- Sviatoslav Voloshynovskiy, *University of Geneva, Switzerland*
- Z. Jane Wang, *University of British Columbia, Canada*
- Ye Wang, *Mitsubishi Electric Research Laboratories, USA*
- Jim Wayman, *San Jose State University, USA*
- Min Wu, *University of Maryland, USA*
- Wenjun Zeng, *University of Missouri, USA*
- Vicky H. Zhao, *University of Alberta, Canada*
- Yihai Zhu, *University of Rhode Island, USA*

WIFS 2015 Organization

Organized by

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Technically Co-Sponsored by

IEEE

IEEE
Signal Processing Society

IFS
IEEE

IEEE
Biometrics Council

EURASIP

Sponsors

Gold

Silver

Bronze

WIFS 2015 Venue

WIFS 2015 is held at the Rectoratus of Roma Tre University, Via Ostiense 159, 00146, Rome, Italy.

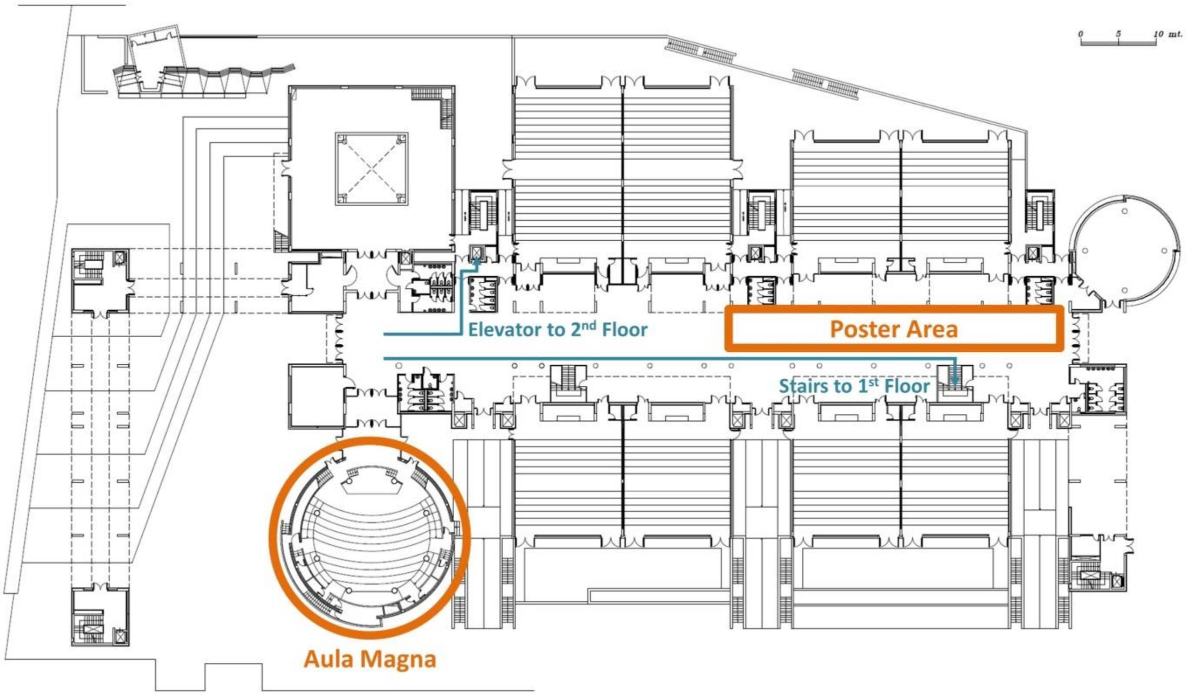
Keynotes are given in the **Aula Magna**.

Tutorials and oral lectures are given in the **Aula Magna** (ground floor) and in the **Aula del Consiglio** (first floor). This latter can be reached through the stairs at end of the foyer of ground floor.

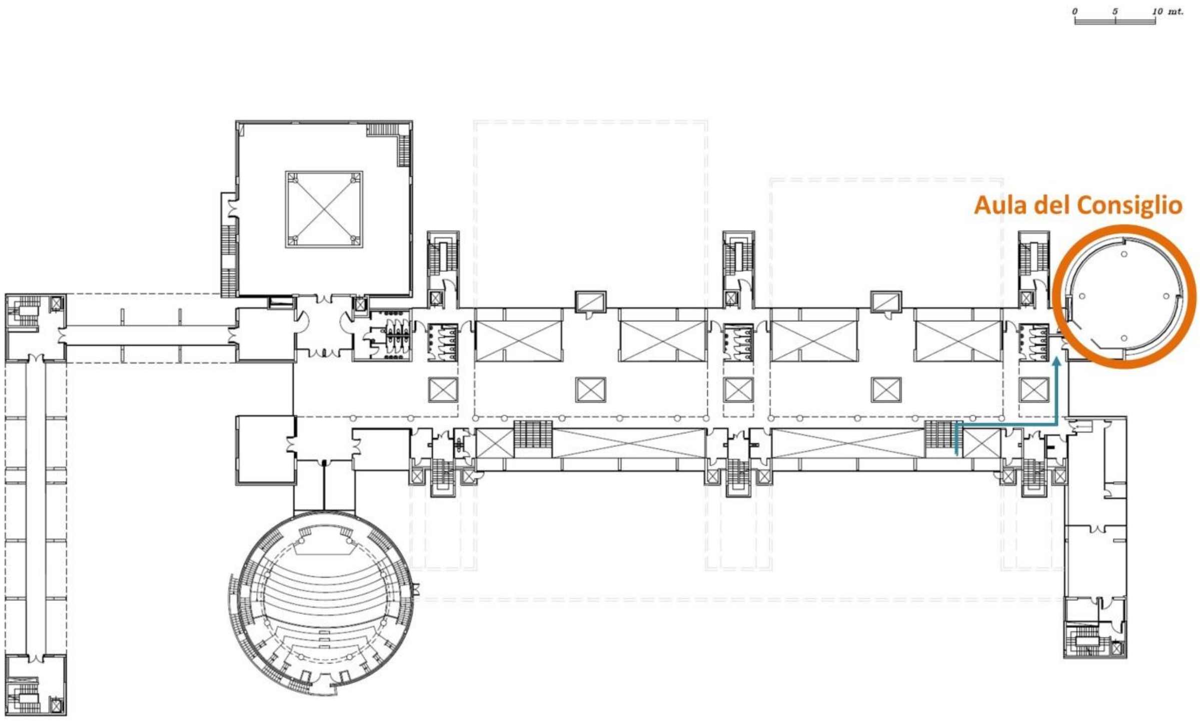
Poster, TIFS/SPL papers and demo/ongoing sessions are held in the **foyer** at ground floor.

Technical and thematic meetings are held in the **Sala del Consiglio del Rettorato** (second floor), reached through the elevator at the beginning of the foyer of ground floor.

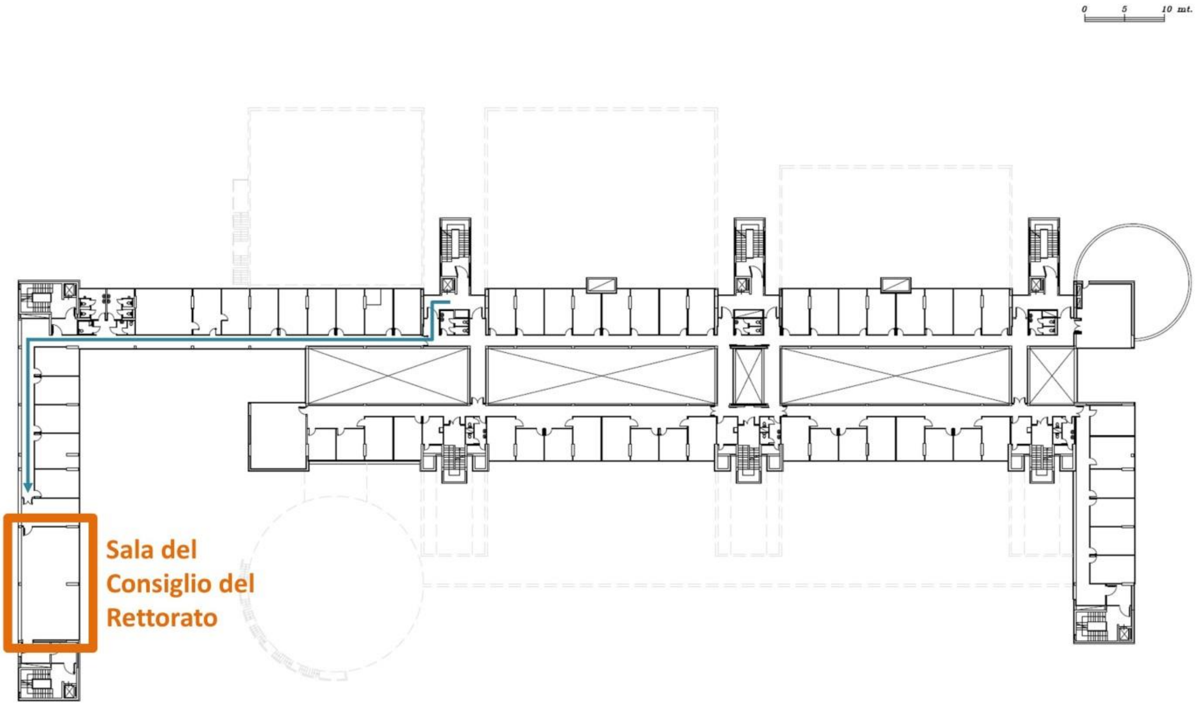
Ground Floor



First Floor



Second Floor



Social Program

Welcome

The Welcome Reception will take place at the workshop venue on Monday, November 16, 2015, at 19:00, after the Tutorials.

Social Event

The social event of Wednesday, November 18, 2015, will include a visit to **Villa Farnesina**, a Renaissance suburban villa placed in Via della Lungara 230, in the district of Trastevere. A bus service will be provided to reach Villa Farnesina from the Workshop venue.

Villa Farnesina is considered one of the noblest and most harmonious creations of Italian Renaissance. At the beginning of the sixteenth century, it was commissioned by the Sienese banker Agostino Chigi to the architect Baldassarre Peruzzi. The interior is decorated with frescoes by Raphael Sanzio, Sebastiano del Piombo, Giovanni da Udine, Giovanni Bazzi known as il Sodoma, Giulio Romano, Giovan Francesco Penni, and Baldassarre Peruzzi himself. At the end of the sixteenth century, the Villa was purchased by Cardinal Alessandro Farnese from whom it takes its name "Farnesina" to distinguish it from Palazzo Farnese on the other side of the Tiber. Accademia Nazionale dei Lincei also uses the Villa for official representative purposes.

For more information, visit http://www.villafarnesina.it/

Gala Dinner

Following the visit to Villa Farnesina, it will be possible to reach by walk the location of the gala dinner, held at the roof garden of the **Grand Hotel de la Minerve**, in Piazza della Minerva 69.

The Grand Hotel de la Minerve, an exclusive five-star Hotel that can give you an authentic thrill, is a jewel set in the heart of ancient Rome, in a building of immense historical and artistic value, with the major attractions in Rome at its doorstep: the Pantheon, Navona square, Trevi Fountain and Spanish Steps among the others.

The hotel's strategic location rewards its guests on the rooftop with a fascinating view. The Minerva Roof Garden, that houses our exclusive Restaurant, treats the palate and seduces its guests with a marvelous 360-degree view of Rome, with its enchanting sunsets.

The Minerva Roof Garden is considered one of the best places in one of the most beautiful places in the world.

For more information, visit http://www.minervaroofgarden.it/

Practical Information

Internet Access

Wi-Fi is free available for all attendees within the Workshop venue. In order to be connected, please use the following networks:

- SSID **Rm3Wi-Fi**; open network, does not require WPA2 security access;
- SSID **Rm3Wi-FiWPA**; requires WPA2 security Access, using the key **Uniroma3WiFi;**
- SSID **EDUROAM**; network available with visitors' own institution credentials.

Both Rm3Wi-Fi and Rm3Wi-FiWPA networks require authentication. The credentials for the workshop attendees are:

- username: **guests_wifs2015**
- password: **Wifs15@UR3**

For further information, please contact the registration desk.

Notice for oral presentation speakers

For oral presentations, speakers need to provide to the session chairs their electronic presentation slides, preferably on an USB device and in .pdf format, before the start of each technical session.

Transportation

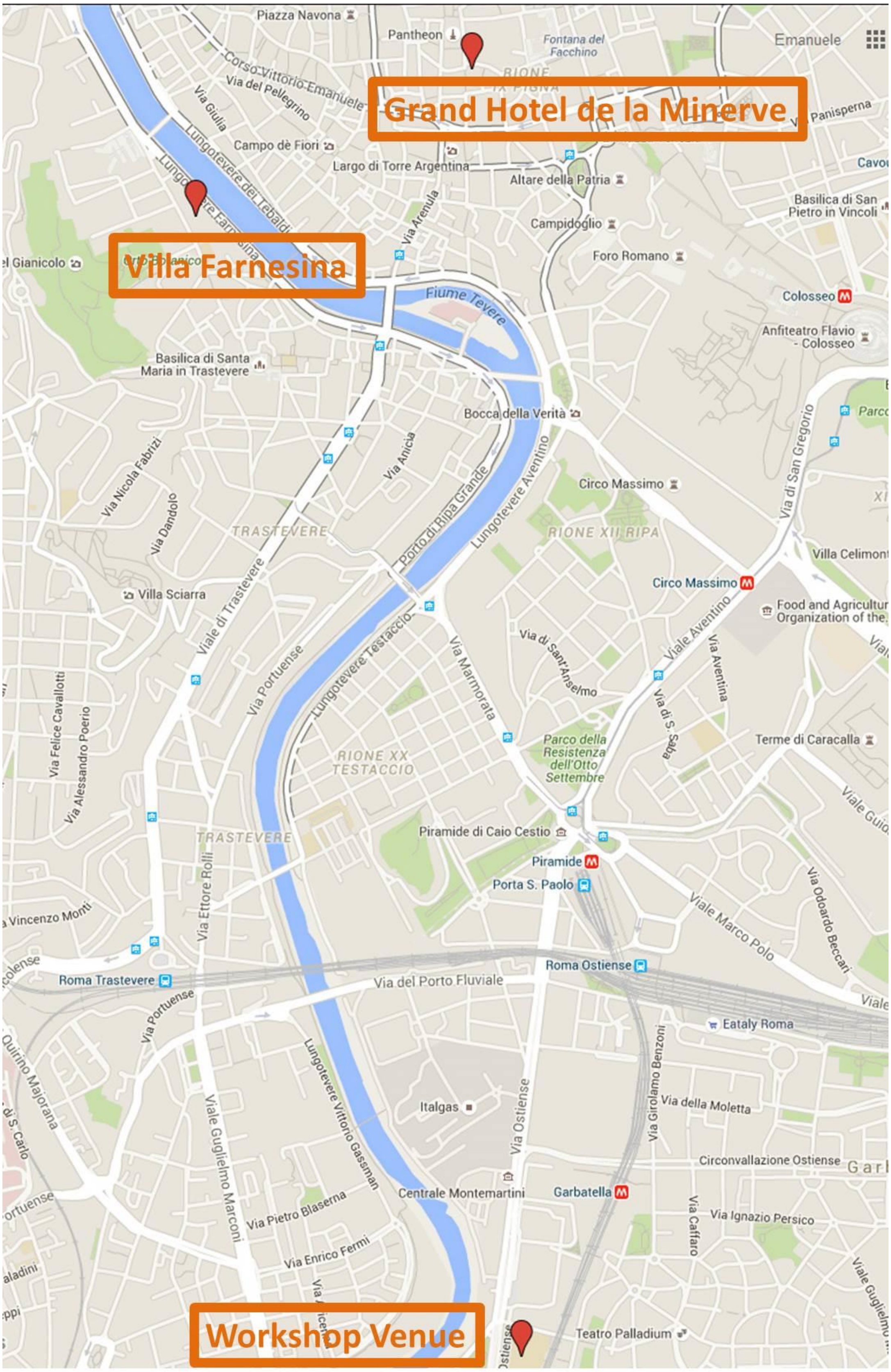
The Workshop venue is located near the Metro station "San Paolo Basilica" on Line B. From there, the center of Rome can be easily reached by arriving at the stations "Circo Massimo, "Colosseo" or "Cavour". Alternatively, Line B can be used to reach "Termini" station, and then changing to Line A to reach "Barberini" or "Spagna" stations.

Rome bus Service, with the Bus 23, can be preferably used in order to go from the workshop venue to Trastevere district (for 13 stops), where the social event is held, and close to the location of the Gala Dinner.

In case a Taxi service is needed, the following companies can be contacted:

• Samarcanda:	+39 065551
• RadioTaxi:	+39 063570
• Pronto Taxi:	+39 066645

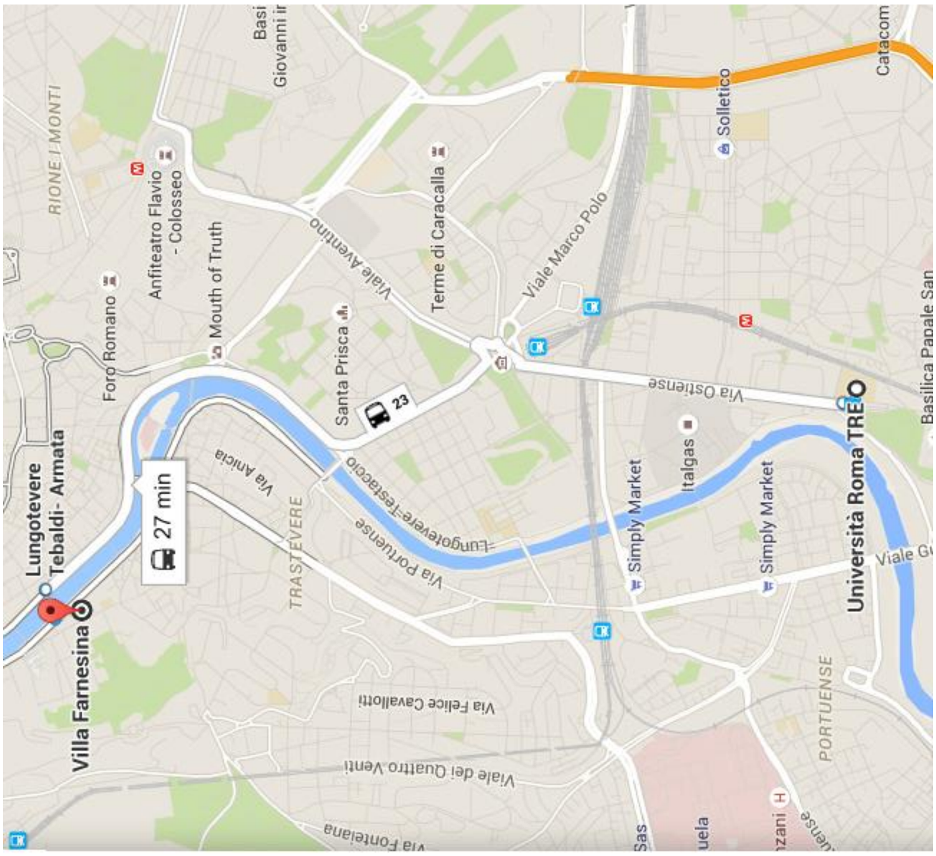
Locations

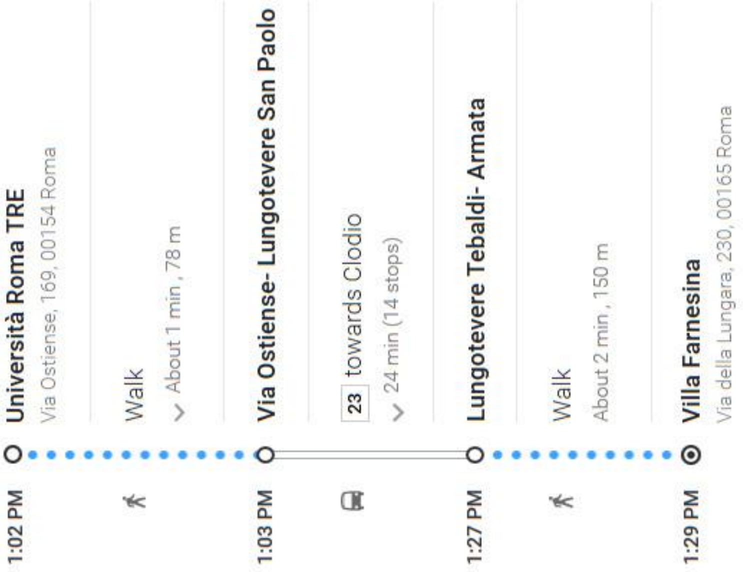

Grand Hotel de la Minerve
Villa Farnesina
Workshop Venue
Piazza Navona
Pantheon
Fontana del Facchino
Emanuele
Corso Vittorio Emanuele
Via del Pellegrino
Via Giulia
Campo dè Fiori
Largo di Torre Argentina
Altare della Patria
Lungotevere dei Tebaldi
Panisperna
Cavou
Basilica di San Pietro in Vincoli
Campidoglio
Foro Romano
Via Arenula
Gianicolo
Colosseo
Anfiteatro Flavio - Colosseo
Fiume Tevere
Basilica di Santa Maria in Trastevere
Bocca della Verità
Parco
Via Nicola Fabrizi
Via Dandolo
Via Anicia
Porto di Ripa Grande
Lungotevere Aventino
Circo Massimo
Via di San Gregorio
TRASTEVERE
RIONE XII RIPA
Villa Celimont
Villa Sciarra
Viale di Trastevere
Circo Massimo
Food and Agricultur Organization of the
Viale Aventino
Via Aventina
Via di Sant'Anselmo
Via Marmorata
Lungotevere Testaccio
Via Portuense
Via Felice Cavallotti
Via Alessandro Poerio
Via di S. Saba
Parco della Resistenza dell'Otto Settembre
Terme di Caracalla
RIONE XX TESTACCIO
TRASTEVERE
Piramide di Caio Cestio
Piramide
Porta S. Paolo
Viale Guid
Via Odoardo Beccari
Viale Marco Polo
Via Ettore Rolli
Vincenzo Monti
Roma Trastevere
Via del Porto Fluviale
Roma Ostiense
Viale
Via Portuense
Eataly Roma
Quirino Majorana
Lungotevere Vittorio Gassman
Italgas
Via Ostiense
Via Girolamo Benzoni
Via della Moletta
Circonvallazione Ostiense
Viale Guglielmo Marconi
Via Pietro Blaserna
Centrale Montemartini
Garbatella
Via Caffaro
Via Ignazio Persico
Via Enrico Fermi
Teatro Palladium
Viale Guglielmo

Directions

From Workshop venue to Villa Farnesina (social event) with Line Bus 23 – 4.8 Km.

A bus service will be provided to reach Villa Farnesina from the Workshop venue.




1:02 PM Università Roma TRE
Via Ostiense, 169, 00154 Roma

Walk
About 1 min , 78 m

1:03 PM Via Ostiense- Lungotevere San Paolo

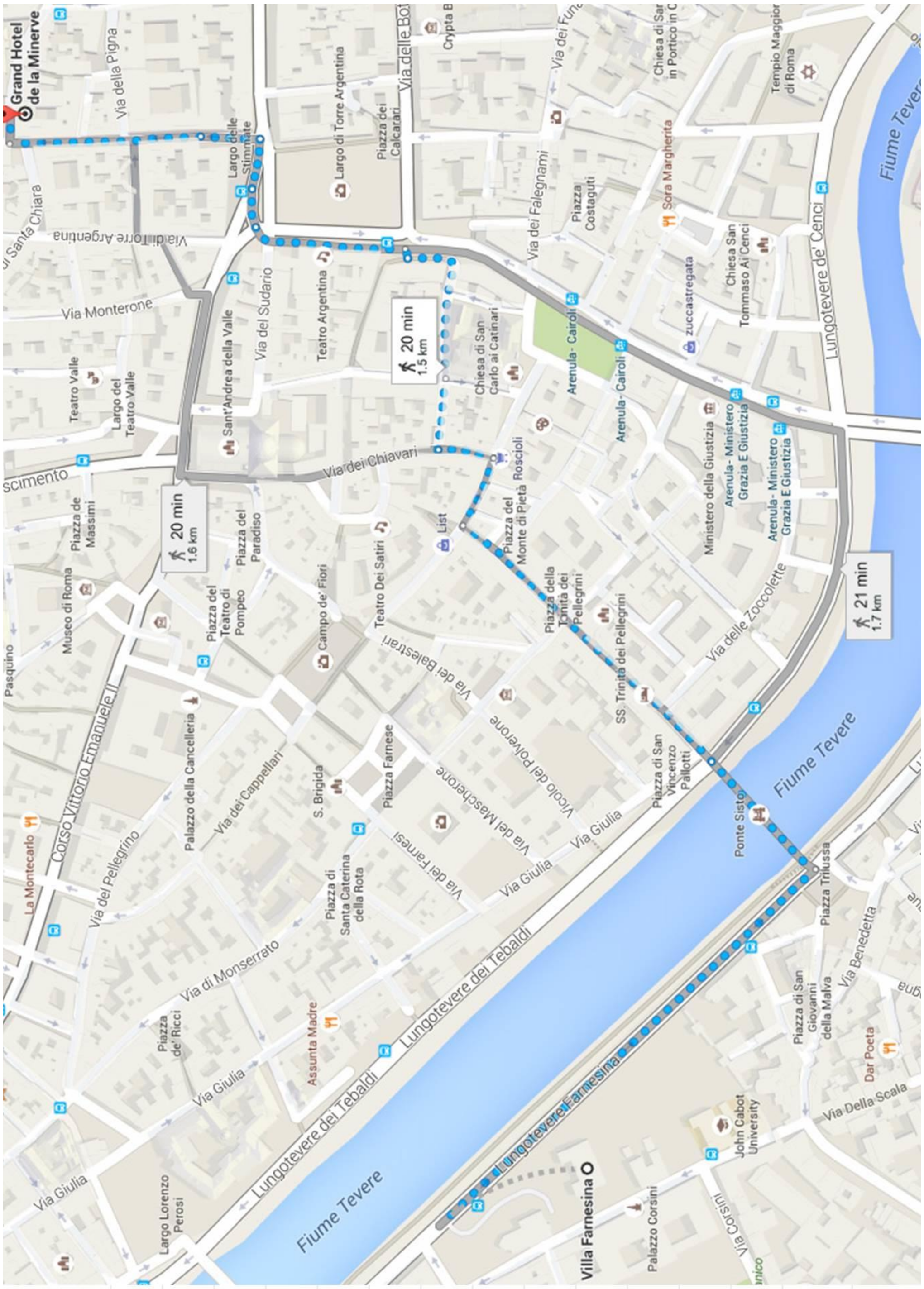
23 towards Clodio
24 min (14 stops)

1:27 PM Lungotevere Tebaldi- Armata

Walk
About 2 min , 150 m

1:29 PM Villa Farnesina
Via della Lungara, 230, 00165 Roma

From Villa Farnesina to Grand Hotel de la Minerve (Gala Dinner) – 1.5 Km

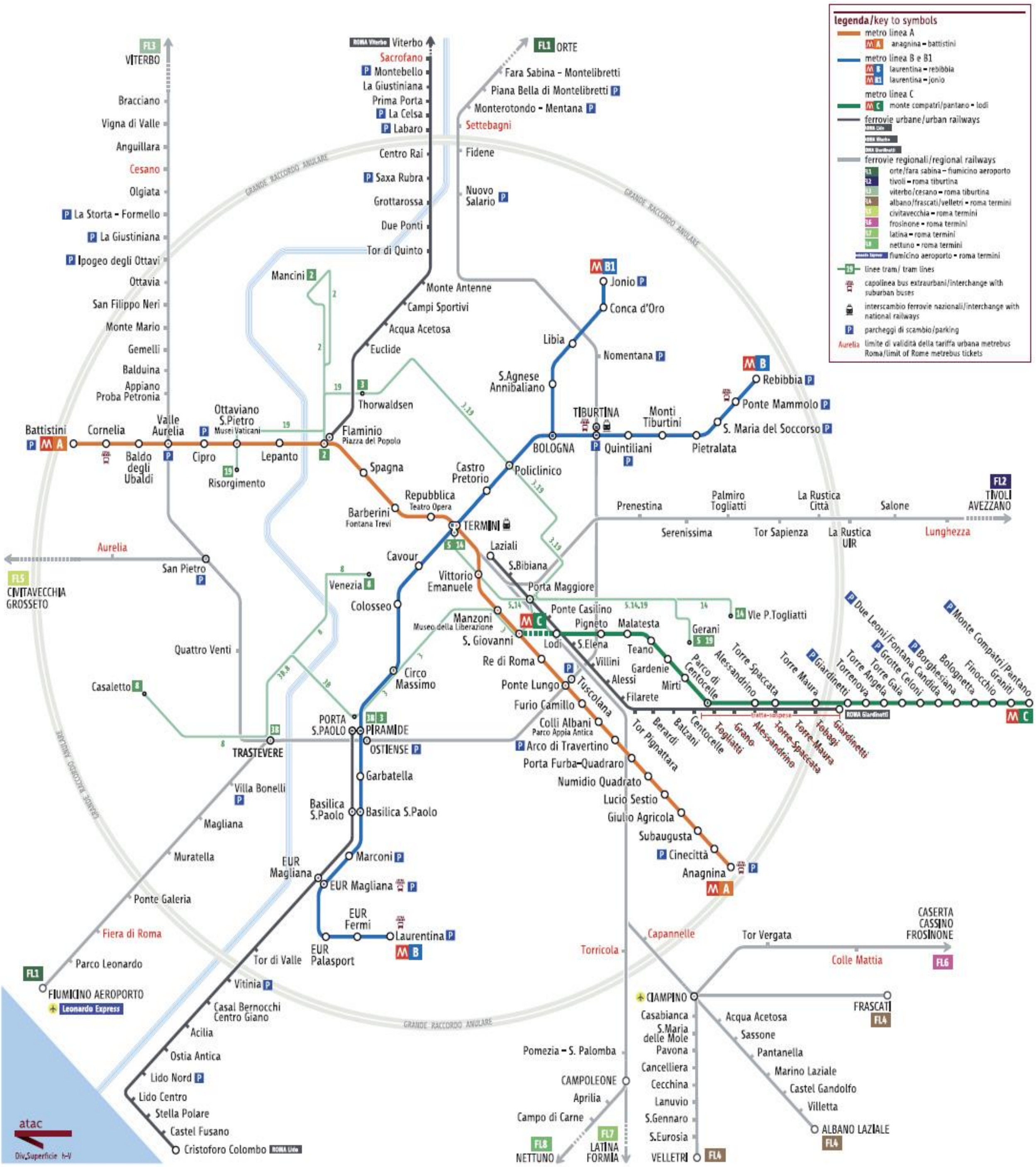


Villa Farnesina
Via della Lungara, 230, 00165 Roma

- ← Head southeast on Lungotevere Farnesina toward Piazza Trilussa — 400 m
- ↰ Turn left onto Ponte Sisto — 120 m
- ← Continue onto Via dei Pettinari — 170 m
- ← Continue onto Via dell'Arco del Monte — 110 m
- ↱ Turn right onto Via dei Giubbonari — 60 m
- ↰ Turn left onto Via dei Chiavari — 45 m
- ↱ Turn right onto Vicolo dei Chiodaroli — 58 m
- ← Continue onto Via di Sant'Anna — 130 m
- ↱ Turn right at Via dei Barbieri — 8 m
- ↰ Turn left onto Largo Arenula — 130 m
- ↱ Slight right onto Largo di Torre Argentina — 32 m
- ← Continue onto Corso Vittorio Emanuele II — 41 m
- ↰ Turn left onto Largo delle Stimmate — 48 m
- ← Continue onto Via dei Cestari — 150 m
- ↱ Turn right onto Piazza della Minerva
  Destination will be on the right — 24 m

Grand Hotel de la Minerve
Piazza della Minerva, 69, 00186 Roma

Rome Metro and Train Services



For larger view, visit: http://romemap360.com/

Tutorials

Monday, 16 November 2015 - Morning Session (Aula Magna)

Privacy-Aware Data Analytics

Shantanu Rane (Palo Alto Research Center, USA)

Big data analytics presents exciting opportunities for individuals, corporations and governments. Applications include discovering elusive treatments and cures, streamlining our transportation systems, securing people and infrastructure against terrorism, distributing and pricing energy in smart grids, driving customer-centric businesses on the internet, and many more. However, the big data requirement appears, almost fundamentally, to conflict with the idea of privacy. Indeed, much of big data analytics today involves indiscriminate information gathering with scant regard for individual privacy. How can expressive analysis be conducted while protecting the privacy of people whose data is collected?

Our objective is to present a systematic overview of privacy-preserving analytics, that exposes the various capabilities, limitations and tradeoffs. We will motivate the need for privacy-aware analytics, by specifying the requirements of stakeholders in the big data analytics setting. Next, we will introduce privacy technologies that have been used to address this problem, including cryptographic techniques (e.g., homomorphic encryption, garbled circuits, searchable encryption, verifiable computing and more), and statistical mechanisms (k-anonymity and its variants, differential privacy). We will highlight the gaps between what can be achieved by existing techniques and what is needed for privacy-aware analytics. In these gaps reside several new challenges for the research community.

Shantanu Rane is a Senior Member of the Research Staff at Palo Alto Research Center (PARC). His research interests are in applied cryptography, signal processing and information theory. He has previously worked at Mitsubishi Electric Research Laboratories (MERL).Shantanu participated in the ITU-T/MPEG H.264/AVC standardization activity, and was an editor and member of the US delegation in the ISO/IEC JTC1 SC37 Subcommittee on Biometrics. He is an associate editor for the IEEE Transactions on Information Forensics and Security and the IEEE Signal Processing Magazine. Shantanu has a Ph.D. in electrical engineering from Stanford University.

Monday, 16 November 2015 - Morning Session (Aula del Consiglio)

Adversarial Signal Processing

Mauro Barni (University of Siena, Italy) and Fernando Pérez-González (University of Vigo, Spain)

Due to rising concerns about security and privacy, and the popularity of cloud-centric services, it has only been recently that the signal processing community has started rethinking designs to account for the presence of a (malicious) adversary. The aim of this tutorial is to present the basic theory of adversarial signal processing, with numerous motivating examples taken from the fields of watermarking, multimedia forensics, traffic analysis, intrusion detection, biometrics, fingerprinting and traitor tracing, reputation systems, cognitive radio, etc. We will focus on adversarial hypothesis testing, which is arguably the best understood topic, and for which the new framework has already produced improved countermeasures. As a fundamental approach, we will show how to use game theory to model the available strategies to both defender and adversary. In some cases of interest, it is possible to find an equilibrium of the game, which gives the optimum strategies for both parties and the performance, that each can achieve.

Contents:

- Introduction and motivation
- Adversarial hypothesis testing
- Game-theoretic approach
- The source identification game
- Applications
- Detecting the presence of the adversary
- Sensitivity, hill climbing and ACRE attacks
- Towards smart detectors
- Challenges and open problems

Mauro Barni graduated in electronic engineering at the University of Florence in 1991. He received the PhD in Informatics and Telecommunications in October 1995. He has carried out his research activity for almost 20 years first at the Department of Electronics and Telecommunication of the University of Florence, then at the Department of Information Engineering and Mathematics of the University of Siena. His research activity focuses on multimedia and information security, with particular reference to copyright protection, multimedia forensics and signal processing in the encrypted domain. He is co-author of almost 300 papers published in international journals and conference proceedings, he holds three patents in the field of digital watermarking and one patent dealing with anticounterfeiting technology. He is co-author of the book "Watermarking

Systems Engineering: Enabling Digital Assets Security and other Applications", published by Dekker Inc. in February 2004. He is editor of the book "Document and Image Compression" published by CRC-Press in 2006. He has been the chairman of the IEEE Multimedia Signal Processing Workshop held in Siena in 2004. He was technical program co-chair of ICASSP 2014. In 2008, he was the recipient of the IEEE Signal Processing Magazine best column award. In 2010 he was awarded the IEEE Transactions on Geoscience and remote sensing best paper award. He was the founding editor in chief of the EURASIP Journal on Information Security. He has been part of the editorial board of several journals. From 2010 to 2011, he has been the chairman of the IEEE Information Forensic and Security Technical Committee of the IEEE Signal Processing Society. He has been a member of the IEEE Multimedia Signal Processing technical committee and of the conference board of the IEEE Signal Processing Society. He was appointed distinguished lecturer by the IEEE Signal Processing Society for the years 2013-2014. He is the Editor in Chief of the IEEE Transactions on Information Forensics and Security. Mauro Barni is a fellow member of the IEEE and senior member of EURASIP.

Fernando Pérez-González received the Ph.D. in Telecommunications Engineering in 1993. He is currently Full Professor at the University of Vigo, Spain, and Research Professor at the University of New Mexico. His research interests lie in the crossroads of signal processing, security/privacy and communications, in particular, those problems in which an adversary is present. Fernando has coauthored more than 200 journal and conference papers, 15 patents, and has participated in 5 European projects related to multimedia security. He has served in the Editorial Board of several international journals, including IEEE Trans. on Information Forensics and Security. He has been in the program committee of more than 100 conferences and workshops.

Monday, 16 November 2015 - Afternoon Session (Aula Magna)

Privacy in Smart Metering Systems

Deniz Gunduz (Imperial College London, London, United Kingdom) and Georgios Kalogridis (Toshiba Telecommunications Research Laboratory in Bristol, UK)

For efficient and reliable electrical energy generation, distribution and demand side management, advanced control mechanisms have been introduced into the Smart Grid (SG). Smart electricity meters (SMs) are an essential component of the SG; they establish a two-way communication infrastructure and enable demand side management by responding to real-time pricing. However, SM readings can also reveal users' habits and behaviors as every electric appliance has its own detectable power consumption signature. Non-intrusive load monitoring techniques can be used for surveillance of users' activities in real-time. Hence, there is a significant tension between sharing data to empower SG mechanisms, and consumer privacy. Further, SM communications are vulnerable to security attacks spoofing or manipulating data and control messages, the orchestration of which at a large scale, may stress or crash the entire power network. This tutorial will provide a comprehensive overview of growing privacy threats to SMs and the smart grid in general. Potential attacks and their impact on the grid, and various privacy preservation solutions will be reviewed. We will provide both an academic and an industry perspective on the future of SMs, and the tools that can be employed to guarantee advanced SM functionality without threatening user privacy.

Deniz Gunduz received M.S. and Ph.D. degrees from NYU Polytechnic School of Engineering in 2004 and 2007, respectively. He held various positions at Princeton University, Stanford University, and CTTC (Spain). Currently, he is a Lecturer at Imperial College London. He is an Editor of the IEEE Transactions on Communications, and IEEE Journal on Selected Areas in Communications Series on Green Communications and Networking. He is the recipient of the 2014 IEEE Communications Society Best Young Researcher Award for the Europe, Middle East, and Africa Region, and the Best Student Paper Award at the 2007 IEEE International Symposium on Information Theory (ISIT).

Georgios Kalogridis received the Dipl. El. Comp. Eng. from the University of Patras, Greece, in 2000, the M.Sc. degree in Advanced Computing from the University of Bristol, U.K., in 2001, and the Ph.D. degree in Mathematics from Royal Holloway, University of London, U.K., in 2011. He is a Principal Research Engineer and a Team Leader at Toshiba Telecommunications Research Laboratory, where he has been working since 2001. His research has spanned the areas of information security, data privacy, machine learning, wireless networking and smart grid communications. In these areas, he has authored papers, invented patents, developed corporate technology prototypes, and contributed to collaborative research projects and standards.

Monday, 16 November 2015 - Afternoon Session (Aula del Consiglio)

The Open Set Recognition Problem in Information Forensics and Security

Walter J. Scheirer (University of Notre Dame, US) and Anderson Rocha (University of Campinas, Brazil)

Coinciding with the rise of large-scale statistical learning within the information forensics and security community there has been a dramatic improvement in automated methods for digital image forensics, forensic linguistics, network intrusion detection, and human biometrics, among many other applications. Despite this progress, a tremendous gap exists between the performance of automated methods in the laboratory and the performance of those same methods in the field. A major contributing factor to this is the way in which machine learning algorithms are typically evaluated: without the expectation that a class unknown to the algorithm at training time will be experienced during operational deployment. The purpose of this tutorial is to introduce the WIFS audience to the open set recognition problem. A number of different topics will be explored, including supervised machine learning, probabilistic models, kernel machines, the statistical extreme value theory, and original case studies related to the topics of interest at WIFS. The tutorial is composed of three parts, each lasting approximately one hour:

- An introduction to the open set recognition problem?
- Algorithms that minimize the risk of the unknown
- Case studies related to images, text and network traffic

Walter J. Scheirer, Ph.D. is an Assistant Professor in the Department of Computer Science and Engineering at the University of Notre Dame. Prior to Notre Dame, he was a Postdoctoral Fellow in the Center for Brain Science at Harvard University. He received his Ph.D. from the University of Colorado and his M.S. and B.A. degrees from Lehigh University. Dr. Scheirer has extensive experience in the areas of security, computer vision and human biometrics, with an emphasis on advanced learning techniques. His overarching research interest is the fundamental problem of recognition, including the representations and algorithms supporting solutions to it.

Anderson Rocha received his B.Sc degree from Federal University of Lavras, Brazil in 2003. He received his M.S. and Ph.D. from University of Campinas, Brazil in 2006 and 2009, respectively. Currently, he is an Associate Professor in the Institute of Computing, Unicamp, Brazil. His main interests include digital image and video forensics, pattern analysis, machine learning, and reasoning for complex data. He is an elected member of the IEEE IFS-TC and was co-general chair of WIFS 2011. In 2011, he was named a Microsoft Research Faculty Fellow. Finally, he is an associate editor for IEEE T-IFS.

Keynote Lectures

Tuesday, 17 November 2015

Smoking Blocks - Fighting and Preventing Crime with Virtual Currencies

Rainer Böhme (Institute of Computer Science, Universität Innsbruck, Austria)

The raise of cryptographic currencies, such as Bitcoin, has arguably benefited from early adoption by criminals who helped to reach critical mass. In this talk, I summarize our research at the intersection of cryptographic currencies and cybercrime. I present approaches to block chain forensics, taking into account the anonymization techniques currently in use, and outline a prevention strategy that might deter criminal use without substantially affecting the potential of legitimate applications of this innovative technology.

Rainer Böhme is Professor of Security and Privacy at the Institute of Computer Science, Universität Innsbruck, Austria. A common thread in his scientific work is the interdisciplinary approach to solving exigent problems in information security and privacy, specifically concerning cyber risk, digital forensics, cyber crime, and crypto finance. Prior affiliations in his academic career include TU Dresden and Westfälische Wilhelms-Universität Münster (both in Germany) as well as the International Computer Science Institute in Berkeley, California.

Wednesday, 18 November 2015

Privacy and Security in the Genomic Era

Jean-Pierre Hubaux (EPFL, Lausanne, Switzerland)

Genome sequencing technology has advanced at a rapid pace and it is now possible to generate highly detailed genotypes inexpensively. The collection and analysis of such data has the potential to support various applications, including personalized medical services. The benefits of the genomics revolution are trumpeted by the biomedical community. Yet, the increased availability of such data has major implications for personal privacy and security, notably because the genome has certain essential features, which include (i) an association with traits and certain diseases, (ii) identification capability (e.g., forensics), and (iii) revelation of family relationships. Moreover, direct-to-consumer DNA testing increases the likelihood that genome data will be made available in less regulated environments, such as the Internet and for-profit companies. The problem of genome data privacy thus resides at the crossroads of computer science, medicine, and public policy. While the computer scientists have addressed data privacy for various data types, there has been less attention dedicated to genomic data. In this talk, we will introduce some basic knowledge on genomics and summarize the main challenges on the front of privacy and security. We will then explain the implications of the laws of heredity on kin genome privacy and provide an overview of the envisioned protection techniques relying notably on homomorphic and honey encryption. More information about genome privacy and security can be found at: https://genomeprivacy.org

Jean-Pierre Hubaux is a full professor at EPFL. Through his research, he contributes to laying and developing the tools to protect privacy in tomorrow's hyper-connected world. He focuses notably on data protection and on network privacy and security. He also studied privacy and security mechanisms (especially for mobile networks) in the presence of selfish players. He pioneered the areas of wireless network security, secure vehicular communications, and genomic privacy. He was an Associate Editor (AE) of IEEE Transactions on Mobile Computing and is an AE of Foundations and Trends in Privacy and Security. He is a Fellow of both IEEE and ACM. Since 2007, he has been one of the seven commissioners of the Swiss FCC. He was recently appointed to the "Information Security Task Force", set up by the Swiss federal government. He is also a member of the "Genomics" task force set up by the Cantonal Ministry of Health and of the scientific advisory board of Sophia Genetics. More about him can be found here: http://people.epfl.ch/jean-pierre.hubaux

Thursday, 19 November 2015

Dealing with noisy data in biometrics and PUFs

Boris Škorić (Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Netherlands)

Biometrics and Physical Unclonable Functions (PUFs) have a lot in common. They require measurement of a physical system, signal processing, and a secure way to obtain robust bit strings from noisy data. Secure error correction is usually done by applying a Fuzzy Extractor or a Secure Sketch, algorithms collectively known as Helper Data Schemes. This talk gives a personal view on recent developments and open challenges regarding the design of Helper Data Schemes, touching on security/privacy performance as well as practicality.

Boris Škorić received a PhD in theoretical physics from the University of Amsterdam, the Netherlands, in 1999. From 1999 to 2008 he was a research scientist at Philips Research, working first on display physics and later on security topics. In 2008 he joined the department of Mathematics and Computer Science at Eindhoven University of Technology, the Netherlands, as assistant professor. His research interests include biometrics, PUFs, traitor tracing, information theory, subjective logic, and the use of quantum physics for security.

Thematic Meeting

Monday, 16 November 2015, 14:15-18:30

Multimedia Truthfulness Verification in Legal Environment and Social Media

M. Barni (University. of Siena), A. Piva (University of Florence), A. De Rosa (University of Florence)

Truthfulness and trustworthiness verification of multimedia objects like audio tracks, digital images and video sequences has or should have a key role in our daily life. Audio-visual data are nowadays valuable sources of information: due to the diffusion of digital devices able of easily acquiring audio tracks and visual contents, each of us may become an active participant in the production of knowledge; furthermore, internet and social media make this knowledge shared and distributed. We can say that we live in a network of sensors, network of people, network of knowledge.

The quality of information in this new scenario changes its meaning and its verification process, due to the multimedia form of the information and its networked sharing. Multimedia data can be easily manipulated and false information easily disseminated on the web, thus making difficult to understand if digital information are a trustworthy representation of reality. Advanced technologies coming from the Multimedia Forensics have been successfully proposed in the last decade for restoring trust in multimedia data: by studying the history of audio-visual contents, such scientific methods provide useful information on the origin of such data as well as on the modifications they have suffered.

Although the awareness of truthfulness of what we see should be always important, in some scenarios it becomes mandatory to allow the exploitation of user-generated contents as source of information. In particular, we focus on two critical scenarios: the legal environment in which audio-visual data are more and more considered as potential digital evidences, and the social media that allows the democratic participation to the generation of information.

To make Multimedia Forensics effective for the trustworthiness verification of multimedia data in real contexts as the legal and the social, its application should be adapted to such practical scenarios far from the ideal laboratory conditions usually considered by researchers: to this aim the first step is to promote the communication between the different players involved in the legal and social environments, in order to collect the particular requirements and constraints dictated by end-users and their operational framework. E.g. scientific methodologies must be compatible with the requirements for digital evidence examination and admission to a court of law; e.g. the process to verify the quality of information in a social media must consider a bottom-up approach involving the social potential.

The thematic meeting will thus be organized as an open discussion, in which the different components from the legal, social and technological parts will share their expertise, questions, requirements.

Program

14:15	Opening	M. Barni and A. Piva
14:30	Technologies	A short introduction to Multimedia Forensics: the science discovering the history of multimedia contents (S. Battiato, Univ. of Catania)
15:00	Legal Environment	15.00: The point of view of Law Enforcement Agencies (G. Tessitore, Servizio Polizia Scientifica) 15.20: The point of view of Court of Law (F. Sarzana di S.Ippolito, Sarzana & Partners Law Firm) 15.40: The point of view of Industries (C.-T. Li, Functional Technologies Ltd) 16.00: Standards and Guidelines for authenticity verification (M. Fontani, FORLAB)
16:20	Coffee Break	
16:50	Social Media	16.50: Social Media and News (J. Spangenberg, Deutsche Welle & REVEAL project) 17.20: Web and Social Media Verification (M. Zampoglou, CERTH-ITI)
17:40	Panel	Moderators: M. Barni and A. Piva
18:30	Closing	M. Barni and A. Piva

Technical Meetings

Tuesday, 17 November 2015, 12:30-14:00

IEEE Transactions on Information Forensics and Security Editorial Board Meeting

Held in the Sala del Consiglio del Rettorato

Wednesday, 18 November 2015, 12:30-14:00

Information Forensics and Security Technical Committee (IFS – TC)

Held in the Sala del Consiglio del Rettorato

IEEE Signal Processing Society Chapter Meeting

Tuesday, 17 November 2015, 18:30-21:00

The IEEE Signal Processing Chapter meeting is meant mainly to promote the SPS among students, both at the undergraduate and the graduate level, with emphasis on female students attending the engineering courses at the regional level, to promote the value of SPS membership among professionals and companies, and to enhance the interaction between industrial entities and academics.

At the same time, the initiative is a driver to stimulate the active participation of SPS members in the initiatives carried out by the IEEE Signal Processing Society.

The meeting will be divided into two parts. In the first one, a panel of speakers, executives coming from industries and academic personalities, will address some issues of interest to students, young professionals, engineers, and the SPS community in general. The second part will be devoted to social networking where academic and company leaders can get together and interact with young professionals and students. A cocktail and light buffet dinner, kindly offered by the IEEE Signal Processing Society, will be given during the networking session.

Participants:

Telecom Italia –TIM, Italy: Dr. Gariela Syf
Technicolor R&D France: Dr. Gwenaël Doërr
Green Bit, Italy: Dr. Sergio Rainero
Gradiant - University of Vigo, Spain: Prof. Fernando Pérez-González

Technical Program

Monday, 16 November 2015

10:00-12:30: Half-Day Tutorials

Tutorial 1: Privacy-aware Data Analysis (Aula Magna)
Shantanu Rane (Palo Alto Research Center, USA)

Tutorial 2: Adversarial Signal Processing (Aula del Consiglio)
Mauro Barni (University of Siena, Italy) and Fernando Pérez-González (University of Vigo, Spain)

12:30-14:00: Lunch

14:00-16:30: Half-Day Tutorials

Tutorial 3: Privacy in Smart Metering Systems (Aula Magna)
Deniz Gunduz (Imperial College London, London, United Kingdom) and Georgios Kalogridis (Toshiba Telecommunications Research Laboratory in Bristol, UK)

Tutorial 4: The Open Set Recognition Problem in Information Forensics and Security (Aula del Consiglio)
Walter J. Scheirer (University of Notre Dame, US) and Anderson Rocha (University of Campinas, Brazil)

18:30-20:30: Welcome Reception

Tuesday, 17 November 2015

9:00- 9:20: **Welcome** (Aula Magna)

9:20-10:40: **Oral session: Biometrics I** (Aula Magna)
Chair: Andreas Uhl (University of Salzburg, Austria)

9:20- 9:40: **Detection and Segmentation of Latent Fingerprints.**
Xiao Yang (Tsinghua University, China), Jianjiang Feng (Tsinghua University, China), Jie Zhou (Tsinghua University, China) and Shutao Xia(Tsinghua University, China)

Latent fingerprints have been used by law enforcement agencies to identify suspects for a century. However, because of poor image quality and complex background noise, latent fingerprints are routinely identified relying on features manually marked by human experts in practice. A large number of latent fingerprints cannot be treated in time due to lacking well trained experts, highlighting the need for "lights out" (fully-automatic) systems. In this paper, we propose a systematic algorithm for latent fingerprint detection, segmentation, and orientation field estimation, without any manual markup. Multiple potential latent fingerprints are detected using a sequential pose estimation algorithm. Then, the full orientation field and confidence map of each detected fingerprint are estimated based on localized dictionaries lookup. Finally, the boundary of each latent fingerprint is delineated by analyzing its confidence map. Experiments on a multi-latent fingerprint database and the challenging NIST SD27 latent fingerprint database show the effectiveness of the proposed algorithm.

9:40-10:00: **Local Gabor Rank Pattern (LGRP): A Novel Descriptor for Face Representation and Recognition.**
Abhishek Gangwar (Center for Development of Advanced Computing, India) and Akanksha Joshi (Center for Development of Advanced Computing, India)

The Gabor filters are considered one of the best image representation approaches for face recognition (FR). Researchers have exploited various configurations of Gabor magnitude as well as Gabor phase responses and their modeling with other descriptors. In this paper, we propose a novel face representation approach; Local Gabor Rank Pattern (LGRP), which exploits ordinal ranking of Gabor responses images. To take advantage of both magnitude and phase parts, we derived, local Gabor Magnitude Rank

Pattern (LGMRP) and local Gabor Phase Rank Pattern (LGPRP) descriptors. We also assigned different weights for different LGRPs using variance measure of Gabor coefficients. The descriptors are formed using regional histograms extracted from encoded Gabor filter responses. Furthermore, the LGMRP and LGPRP descriptors are combined within a score-level fusion framework to further improve classification accuracy by maximizing the complementary effect. Extensive experiments on standard face benchmark FERET show that the proposed methods outperforms conventional Gabor counterparts as well as other Gabor encoding methods in both constrained and unconstrained FR. The proposed methods also achieve comparable performance to state-of-the-art descriptor based methods in FR.

10:00-10:20: **Which Dataset is this Iris Image From?**

Susan El-Naggar (West Virginia University, USA) and Arun Ross (Michigan State University, USA)

The performance of a biometric recognition algorithm is often evaluated by testing it on standard datasets. This process, known as technology evaluation, is necessary to compare the matching performance of different algorithms. In the case of iris recognition, datasets such as ICE, MBGC, CASIA, NICE, WVU, UBIRIS, etc. have been used for this purpose. However, iris images in each of these datasets are impacted by the methodology used to collect them. Factors such as external lighting, sensor characteristics, acquisition protocol, subject composition, data collection environment, nuances of the collection process, etc. are dataset-specific and they leave a digital ’imprint’ on the associated data. Therefore, iris images in different datasets may exhibit different intricate characteristics that can potentially impact the performance assessment process. In this work, we conduct an experiment to determine if such dataset-specific attributes are significant enough to be detected in the collected images. To this end we formulate a classification problem where the goal is to determine the dataset to which a given input iris image belongs to. By extracting a set of statistical and Gabor-based features from an iris image, we use a learning-based scheme to associate the input iris image with a specific database. A 83% accuracy is obtained on a set of 1536 images from 8 different datasets collected using 6 different sensors.

10:20-10:40: **Update Strategies for HMM-Based Dynamic Signature Biometric Systems.**

Ruben Tolosana (Universidad Autonoma de Madrid, Spain), Ruben Vera-Rodriguez (Universidad Autonoma de Madrid, Spain), Javier Ortega-Garcia (Universidad Autonoma de Madrid, Spain) and Julian Fierrez (Universidad Autonoma de Madrid, Spain)

Biometric authentication on devices such as smartphones and tablets has increased significantly in the last years. One of the most acceptable and increasing traits is the handwriting signature as it has been used in financial and legal agreements scenarios for over a century. Nowadays, it is frequent to sign in banking and commercial areas on digitizing tablets. For these reasons, it is necessary to consider a new scenario where the number of training signatures available to generate the user template is variable and besides it has to be taken into account the lap of time between them (inter-session variability). In this work, we focus on dynamic signature verification. The main goal of this work is to study system configuration update strategies of time functions-based systems such as Hidden Markov Model (HMM) and Gaussian Mixture Models (GMM). Therefore, two different cases have been considered. First, the usual case of having an HMM-based system with a fixed configuration (i.e. Baseline System). Second, an HMM-based and GMM-based systems whose configurations are optimized regarding the number of training signatures available to generate the user template. The experimental work has been carried out using an extended version of the Signature Long-Term database taking into account skilled and random or zero-effort forgeries. This database is comprised of a total of 6 different sessions distributed in a 15-month time span. Analyzing the results, the Proposed Systems achieve an average absolute improvement of 4.6% in terms of EER(%) for skilled forgeries cases compared to the Baseline System whereas the average absolute improvement for the random forgeries cases is of 2.7% EER. These results show the importance of optimizing the configuration of the systems compared to a fixed configuration system when the number of training signatures available to generate the user template increases.

9:20-10:40: Oral Session: Steganography and Steganalysis (Aula del Consiglio)
Chair: Andrew Ker (Oxford University, UK)

9:20- 9:40: **Side-Informed Steganography with Additive Distortion.**
Tomas Denemark (Binghamton University, USA) and Jessica Fridrich (Binghamton University, USA)

Side-informed steganography is a term used for embedding secret messages while utilizing a higher quality form of the cover object called the precover. The embedding algorithm typically makes use of the quantization errors available when converting the precover to a lower quality cover object. Virtually all previously proposed side-informed steganographic schemes were limited to the case when the side-information is in the form of an uncompressed image and the embedding uses the unquantized DCT coefficients to improve the security when JPEG compressing the precover. Inspired by the side-informed (SI) UNIWARD embedding scheme, in this paper we describe a general principle for incorporating the side-information in any steganographic scheme designed to minimize embedding distortion.

Further improvement in security is obtained by allowing a ternary embedding operation instead of binary and computing the costs from the unquantized cover. The usefulness of the proposed embedding paradigm is demonstrated on a wide spectrum of various information-reducing image processing operations, including image downsampling, color depth reduction, and filtering. Side-information appears to improve empirical security of existing embedding schemes by a rather large margin.

9:40-10.00: **A Sequential Method for Online Steganalysis.**
Rémi Cogranne (Troyes University of Technology, France)

This paper studies online detection of hidden information in digital images. By online, it is meant that we inspect a flow of images that are transmitted sequentially. This has crucial consequences on the detection of hidden data. By contrast to the usual detection settings, the delay before detection has to be considered in the definition of the correct detection probability, or power function. Similarly, the false alarm probability is considered with respect to a number of inspected cover images. In this paper a new sequential detection method is proposed with the goal to maximize the detection accuracy for a prescribed detection delay. The study of proposed sequential test allows the establishing of detection power as a function of detection delay and also permits us to bound the probability of false alarm for a given number of cover images. Numerical results on real image using both the well-known WS type of detector and the recent ensemble classifier show the relevance of the proposed approach and the accuracy of the theoretical findings.

10:00-10:20: **Is Ensemble Classifier Needed for Steganalysis in High-Dimensional Feature Spaces?**
Rémi Cogranne (Troyes University of Technology, France), Vahid Sedighi (Binghamton University, USA), Jessica Fridrich (Binghamton University, USA) and Tomas Pevny (Czech Technical University in Prague, Czech Republic)

The ensemble classifier, based on Fisher Linear Discriminant base learners, was introduced specifically for steganalysis of digital media, which currently uses high-dimensional feature spaces. Presently it is probably the most used method to design supervised classifier for steganalysis of digital images because of its good detection accuracy and small computational cost. It has been assumed by the community that the classifier implements a non-linear boundary through pooling binary decision of individual classifiers within the ensemble. This paper challenges this assumption by showing that linear classifier obtained by various regularizations of the FLD can perform equally well as the ensemble. Moreover it demonstrates that using state of the art solvers linear classifiers can be trained more efficiently and offer certain potential advantages over the original ensemble leading to much lower computational complexity than the ensemble classifier. All claims are supported experimentally on a wide spectrum of stego schemes operating in both the spatial and JPEG domains with a multitude of rich steganalysis feature sets.

10:20-10:40: **Optimizing Pooling Function for Pooled Steganalysis.**
Tomas Pevny (Czech Technical University in Prague, Czech Republic) and Ivan Nikolaev (Cisco systems Inc., Czech Republic)

Pooled steganalysis combines evidence from multiple objects to achieve higher accuracy in detecting hidden messages at the expense of granularity, as the decision is provided on the set of objects instead of a single one. Although it has been introduced almost decade ago, very little work has been done since then. This work builds upon recent advances in machine learning to show, how an optimal function combining outputs of a single object detector on a set of objects can be learned. Although experiments demonstrate that learned combining functions are superior to the prior art, more importantly they reveal many interesting phenomenons and points to direction of further research.

10:40-11:10: Communication Break

11:10-12:30: Oral Session: Robust Hashing (Aula Magna)
Chair: Gwenael Doerr (Technicolor, France)

11:10-11:30: **Multiscale Anisotropic Texture Unsupervised Clustering for Photographic Paper.**
Stephane Roux (ENS Lyon, France), Nicolas Tremblay (ENS Lyon, France), Pierre Borgnat (ENS Lyon, France), Patrice Abry (ENS Lyon, France), Herwig Wendt (IRIT - ENSEEIHT, France) and Paul Messier (LLC Boston, USA)

Texture characterization of photographic papers is likely to provide scholars with valuable information regarding artistic practices. Currently, texture assessment remains mostly based on visual and manual inspections, implying long repetitive tasks prone to inter- and even intra-observer variability. Automated texture characterization and classification procedures are thus important tasks in historical studies of large databases of photographic papers, likely to provide quantitative and reproducible assessments of texture matches. Such procedures may, for instance, produce vital information on photographic prints of uncertain origins. The hyperbolic wavelet transform, because it relies on the use of different dilation factor along the horizontal and vertical axes, permits to construct robust and meaningful multiscale and anisotropic representation of textures. In the present contribution, we explore how unsupervised clustering strategies can be complemented both to assess the significance of extracted clusters and the strength of the contribution of each texture to its associated cluster. Graph based filterbank strategies will notably be investigated with the aim to produce small size significant clusters. These tools will be illustrated at work on a large database of about 2500 exposed and non exposed photographic papers carefully assembled and documented by the MoMA and P. Messier's foundation. Results will be commented and interpreted in close cross-disciplinary interactions amongst the authors.

11:30-11:50: **Secure Modular Hashing.**

Abelino Jimenez (Carnegie Mellon University, USA), Bhiksha Raj (Carnegie Mellon University, USA), Jose Portelo (Instituto Superior Tecnico, Portugal) and Isabel Trancoso (Instituto Superior Tecnico, Portugal)

In many situations, such as in biometric applications, there is need to encrypt and “hide” data, while simultaneously permitting restricted computations on them. We present a method to securely determine the l_2 distance between two signals if they are close enough. This method relies on a locality sensitive hashing scheme based on a secure modular embedding, computed using quantized random projections, being a generalization of previous work in the area. Secure Modular Hashes (SMH) extracted from the signals preserve information about the distance between the signals, hiding other characteristic from the signals. Theoretical properties state that the described scheme provides a mechanism to threshold how much information to reveal, and is also information theoretically secure above this threshold. Finally, experimental results reveal that distances computed from SMH vectors can effectively replace the actual Euclidean distances with minimal degradation.

11:50-12:10: **Counterfeit Detection Using Paper PUF and Mobile Cameras.**

Chau-Wai Wong (University of Maryland, College Park, USA) and Min Wu (University of Maryland, College Park, USA)

This work studies the paper authentication problem by exploiting optical features through mobile imaging devices to characterize the unique, physically unclonable properties of paper surface. Prior work either uses a commodity scanner for estimating a projected normal vector field of the surface of the paper as the feature for authentication, or uses an industrial camera with controlled lighting to obtain an appearance image of the surface as the feature. In comparison, past explorations based on mobile cameras have not had substantial success in obtaining consistent appearance images due to the uncontrolled nature of the ambient light. We show in this work that images captured by mobile cameras can be directly used for authentication by exploiting the camera flashlight to create a semi-controlled lighting condition. We proposed new algorithms to demonstrate that paper's microscopic normal vector field can be estimated by using multiple camera-captured images of different viewpoints. Our findings can relax restricted imaging setups to enable paper authentication under a more casual, ubiquitous setting of a mobile imaging device, which may facilitate duplicate detection of paper documents and merchandise packaging.

12:10-12:30: **Information-Theoretical Limits of Active Content Fingerprinting in Content-based Identification Systems.**
Farzad Farhadzadeh (Eindhoven University of Technology, Netherlands), Frans M. J. Willems (Eindhoven University of Technology, Netherlands) and Sviatoslav Voloshynovskiy (University of Geneva, Switzerland)

Content fingerprinting and digital watermarking are techniques that are used for content protection and distribution monitoring and, more recently, for interaction with physical objects. Over the past few years, both techniques have been well studied and their shortcomings understood. In this paper, we introduce a new framework called active content fingerprinting, which takes the best from these two worlds, i.e., the world of content fingerprinting and that of digital watermarking, in order to overcome some of the fundamental restrictions of these techniques in terms of performance and complexity. The proposed framework extends the encoding process of conventional content fingerprinting such that it becomes possible to extract more robust fingerprints from the modified data. We consider different encoding strategies and examine the performance of the proposed schemes in terms of content identification rate in an information theoretical framework and compare them with those of conventional content fingerprinting and watermarking.

12:30-14:00: Lunch

14:00-15:00: Keynote Talk (Aula Magna)

Smoking Blocks - Fighting and Preventing Crime with Virtual Currencies.
Rainer Böhme (Institute of Computer Science, Universität Innsbruck, Austria)

15:00-16:40: Oral Session: Device Security (Aula Magna)
Chair: Shantanu Rane (Palo Alto Research Center, USA)

15:00-15:20: **Key Search and Adaptation based on Association Rules for Backward Secrecy.**
Kannan Karthik (Indian Institute of Technology Guwahati, India)

Static storage of decryption keys in RFID tags creates a security issue particularly when some of these tags are compromised. To address this problem we propose a framework in which these tags search and compute decryption keys based on specific intrinsic *association rules* embedded in the tags, which feed on publicly known broadcast messages transmitted by the centre. This association rule is nothing but a circular linked list, which connects a set of T tokens in some random order. To facilitate backward secrecy, we also propose a rule adaptation methodology based on random deletions within this circular linked list triggered by random numbers sent by the centre. We have shown theoretically that the search space for tags in possession of the actual keys is linear in the number of tokens contained in the association rule i.e. O(T), while the search space for eavesdropping tags increases considerably to O(T^r), where r is centre-defined as the length of the footprint, within a circular linked list. Tradeoffs which involve balancing the extent of backward secrecy with network lifetime, are discussed.

15:20-15:40: **Reliable Secret Key Generation from Physical Unclonable Functions Under Varying Environmental Conditions.**

Onur Günlü (Technische Universität München, Germany), Onurcan İşcan (Technische Universität München, Germany) and Gerhard Kramer (Technische Universität München, Germany)

Two methods are proposed to extract secret keys from ring oscillator (RO) physical unclonable functions (PUFs) under varying environmental conditions. A discrete cosine transform (DCT)-based RO PUF scheme that gives good results under nominal conditions is used in combination with these two methods, which are shown to be highly robust to environmental variations. The proposed methods significantly improve the number-of-securely-extracted-bits, reliability, uniqueness, and randomness results of existing RO PUF schemes under varying temperature and voltage conditions.

15:40-16:00: **WristSnoop: Smartphone PINs Prediction using Smartwatch Motion Sensors.**

Allen Sarkisyan (California State University Northridge, USA), Ryan Debbiny (California State University Northridge, USA) and Ani Nahapetian (California State University Northridge, USA)

Smartwatches, with motion sensors, are becoming a common utility for users. With the increasing popularity of practical wearable computers, and in particular smartwatches, the security risks linked with sensors on board these devices have yet to be fully explored. Recent research literature has demonstrated the capability of using a smartphone's own accelerometer and gyroscope to infer tap locations; this paper expands on this work to demonstrate a method for inferring smartphone PINs through the analysis of smartwatch motion sensors. This study determines the feasibility and accuracy of inferring user keystrokes on a smartphone through a smartwatch worn by the user. Specifically, we show that with malware accessing only the smartwatch's motion sensors, it is possible to recognize user activity and specific numeric keypad entries. In a controlled scenario, we achieve results no less than 41% accurate with a maximum of 92% accuracy for PIN prediction within 5 guesses.

16:00-16:20: **Continuous Authentication and Identification for Mobile Devices: Combining Security and Forensics.**

Soumik Mondal (Gjøvik University College, Norway) and Patrick Bours (Gjøvik University College, Norway)

In this paper, we consider an additional functionality to continuous authentication which is the identification of an impostor. We use continuous authentication to protect a mobile device. Once it is detected that it is not the genuine user that is using the mobile device, it is important to lock it, but in a closed user group, valuable information could also be gained from determining who the actual person was that was operating the device. This new concept is termed continuous identification and in this paper we will show that we can identify the impostors with almost 98% accuracy in case the security settings are such that an impostor is detected after 15 actions on average. In case of a higher security, we already can detect impostors after 4 actions on the mobile device, but in that case the recognition rate of the correct impostor drops to almost 83%.

16:20-16:40: **Practicability Study of Android Volatile Memory Forensic Research.**

Philipp Wächter (Hochschule Albstadt-Sigmaringen, Germany) and Michael Gruhn (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

As Android device encryption and also application storage encryption becomes more widespread, memory analysis becomes more important. Memory is often the only data immediately accessible without decryption and in most cases stores the encryption keys of persistent data currently in use. This work therefore investigates the practicability of current state of the art forensic methods for acquiring and analyzing the volatile memory of Android smartphones as presented by current research publications. To this end, we investigate 8 different Android smartphones in their stock vendor configurations. While we are able to recreate current research results by specifically preparing specific phones the same way as described in the relevant research publications, we are only able to conduct a full acquisition and full analysis against 1 of our 8 sample smartphones in its stock configuration. Because the stock configuration, as shipped by the manufacturer, i.e. non-rooted and locked boot loader, is the most likely configuration encountered during a real forensic investigation, we unfortunately must conclude that current presented methods are not applicable in practice. We further present reasons for our conclusion and possible resolutions which should be endeavored by future research.

16:40-17:10: Communication Break

17:10-18:30: Poster Session (Foyer)
Chair: Patrick Bas (Ecole Centrale de Lille, France)

- **Rediscovering text in the Yale Martellus Map.**
  Roger Easton (Rochester Institute of Technology, USA), Kevin Sacca (Rochester Institute of Technology, USA), Gregory Heyworth (University of Mississippi, USA), Chet Van Duzer (Map Historian, USA), Kenneth Boydston (Megavision, Inc., USA) and Michael Phelps (Early Manuscripts Electronic Library, USA)

  A world map painted by Henricus Martellus c. 1491 is widely acknowledged to be of great importance in the history of cartography, but has been little studied since it came to the attention of scholars in 1959 because the pigments used to write the descriptive texts and place names has faded or flaked off of the surface. Spectral images of this map collected in August 2014 have been processed by several statistical methods, allowing much of the text to be recovered. The methods may be applied to other documents and for forensic applications.

- **TRAP: using TaRgeted Ads to unveil Google personal Profiles.**
  Mauro Conti (University of Padua, Padua, Italy), Vittoria Cozza (Institute of Informatics and Telematics of CNR, Pisa, Italy), Marinella Petrocchi (Institute of Informatics and Telematics of CNR, Pisa, Italy) and Angelo Spognardi (Institute of Informatics and Telematics of CNR, Pisa, Italy)

  In the last decade, the advertisement market spread significantly in the web and mobile app system. Its effectiveness is also due thanks to the possibility to target the advertisement on the specific interests of the actual user, other than on the content of the website hosting the advertisement. In this scenario, became of great value services that collect and hence can provide information about the browsing user, like Facebook and Google. In this paper, we show how to maliciously exploit the Google Targeted Advertising system to infer personal information in Google user profiles. In particular, the attack we consider is external from Google and relies on combining data from Google AdWords with other data collected from a website of the Google Display Network. We validate the effectiveness of our proposed attack, also discussing possible application scenarios. The result of our research shows a significant practical privacy issue behind such type of targeted advertising service, and call for further investigation and the design of more privacy-aware solutions, possibly without impeding the current business model involved in online advertisement.

- **Reconstruction of Smartphone Images for Low Resolution Iris Recognition.**
  Fernando Alonso-Fernandez (Halmstad University, Sweden), Reuben Farrugia (University of Malta, Malta)and Josef Bigun (Halmstad University, Sweden)

  As iris systems evolve towards a more relaxed acquisition, low image resolution will be a predominant issue. In this paper we evaluate a super-resolution method to reconstruct iris images based on Eigen-transformation of local image patches. Each patch is reconstructed separately, allowing better quality of enhanced images by preserving local information. We employ a database of 560 images captured in visible spectrum with two smartphones. The presented approach is superior to bilinear or bicubic interpolation, especially at lower resolutions. We also carry out recognition experiments with six iris matchers, showing that better performance can be obtained at low-resolutions with the proposed eigen-patch reconstruction, with fusion of only two systems pushing the EER to below 5-8% for down-sampling factors up to a size of only 13x13.

- **Improved Edit Detection in Speech via ENF Patterns.**
  Paulo Antonio Andrade Esquef (National Laboratory for Scientific Computing, Brazil), José Antônio Apolinário Jr. (Military Institute of Engineering, Brazil) and Luiz Wagner P. Biscainho (Federal University of Rio de Janeiro & PEE/COPPE UFRJ, Brazil)

  In a recent paper published in the IEEE TIFS, we proposed an edit detection method based on the instantaneous variations of the Electrical Network Frequency (ENF). In this work we modify the detection criteria of that method by taking advantage of the typical pattern of ENF variations elicited by audio edits. We describe the implemented modifications and directly confront the performance of both methods using two distinct signal databases that contain real-life speech recordings. The experimental results demonstrate that the new proposition has an improved performance in terms of lower equal error rates when compared to its former version.

- **Fast Target Link Flooding Attack Detection Scheme by Analyzing Traceroute Packets Flow.**
  Takayuki Hirayama (Keio University, Japan), Kentaroh Toyoda (Keio University, Japan and Iwao Sasase (Keio University, Japan

  Recently, a botnet based DDoS (Distributed Denial of Service) attack, called target link fooding attack, has been reported that cuts off specifc links over the Internet and disconnects a specifc region from other regions. Detecting or mitigating the target link fooding attack is more diffcult than legacy DDoS attack techniques, since attacking flows do not reach the target region. Although many mitigation schemes are proposed, they detect the attack after it occurs. In this paper, we propose a fast target link flooding attack detection scheme by leveraging the fact that the traceroute packets are increased before the attack caused by the attacker's reconnaissance. Moreover, by analyzing the characteristic of the target link flooding attack that the number of traceroute packets simultaneously increases in various regions over the network, we propose a detection scheme with multiple detection servers to eliminate false alarms caused by sudden increase of traceroute packets sent by legitimate users. We show the effectiveness of our scheme by the computer simulation.

- **Splicebuster: a new blind image splicing detector.**
  Davide Cozzolino (University Federico II of Naples, Italy), Giovanni Poggi (University Federico II of Naples, Italy) and Luisa Verdoliva (University Federico II of Naples, Italy)

  We propose a new feature-based algorithm to detect image splicings without any prior information. Local features are computed from the co-occurrence of image residuals and used to extract synthetic feature parameters. Splicing and host images are assumed to be characterized by different parameters. These are learned by the image itself through the expectation-maximization algorithm together with the segmentation in genuine and spliced parts. A supervised version of the algorithm is also proposed. Preliminary results on a wide range of test images are extremely encouraging, showing that a limited-size, but meaningful, learning set may be sufficient for reliable splicing localization.

- **VSig: Hand-Gestured Signature Recognition and Authentication with Wearable Camera.**
  Hasan Sajid (University of Kentucky, USA) and Sen-Ching Samson Cheung (University of Kentucky, USA)

  Wearable camera is gaining popularity not only as a recording device for law enforcement and hobbyists, but also as a human-computer interface for the next generation wearable technology. It provides a more convenient and portable platform for gesture input than stationary camera, but poses unique challenges due to user movement and scene variation. In this paper, we describe a robust wearable camera based system called VSig for hand-gestured signature recognition and authentication. The proposed method asks the user to virtually sign within the field of the view of the wearable camera. Fingertip is segmented out and tracked to reconstruct the signature. This is followed by signature matching for authentication with the pre-stored signatures of the individual. A dataset named SIGAIR comprising of hand-gestured signatures from 10 individuals has been created and used for testing. An average accuracy of 97.5% is achieved by the proposed method.

17:10-18:30: Demo/Ongoing Session (Foyer)
Chair: Samson Cheung (University of Kentucky, USA)

- **Motion Detection for Surveillance Videos on Encrypted H.264/AVC Bitstream** (Ongoing Work)
  Jianting Guo (Sun Yat-Sen University, China), Peijia Zheng (Sun Yat-Sen University, China) and Jiwu Huang (Shenzhen University, China)

  For a cloud-based surveillance system, sending the plaintext videos to the cloud may leak user's privacy. Existing cloud-based motion detection algorithms are performed on the video frames and not suitable for the encoded videos which are usually exploited. In this paper, we propose a motion detection scheme for encrypted surveillance videos in the cloud, to protect the user's privacy. Different from the previous works, the videos are being encrypted directly in the H.264/AVC bitstream, rather than being decoded into frames to which the encryption being applied. The proposed motion detection algorithm is then performed on the encrypted H.264/AVC bitstream, without decryption and video decoding. For this reason, we believe the proposed scheme has the advantage of privacy-preserving and practically feasible over the other schemes. We conduct some experiments to test our algorithm. The experimental results show that the detection performance is comparable to the existing works.

- **Analysis of Streaming Parameters in Hybrid Video Surveillance Systems** (Ongoing Work)
  Angelo Cardellicchio (Politecnico di Bari, Italy), Vito Renò (CNR, Italy) and Cataldo Guaragnella (Politecnico di Bari, Italy)

  The constantly growing number of mobile devices, equipped by high processing capabilities and quality cameras, is pushing the interest of the computer vision scientific community toward new and powerful applications based on the crowdsourced acquisition of ideo content from mobile cameras, in the general framework of smart cities/communities. The possibility to integrate the mobile user cameras into video surveillance systems is a powerful and interesting topic facing several challenges related to the network congestion, the differences in image quality and video formats and the distribution of the computational load. In this paper we address the problem of the fine tuning of a heterogeneous surveillance system when dealing with different video codecs, picture size, resolution, noise and internet access in order to understand which are the best parameters to set up a Hybrid Video Surveillance System (HVSS). In this scenario, this is a fundamental step toward the development of a fully operational cooperative, distributed and crowdsourced video surveillance system.

- **Visual Bubble Based Privacy Protection** (Demo)
  Shaoqian Wang (University of Kentucky, USA) and Samson Cheung (University of Kentucky, USA)

  Wearable cameras are increasing used in many different applications from law enforcement to medicine. Their privacy concerns vary among different applications, and can be quite different from those of stationary surveillance cameras. In this paper, we consider the application of using a wearable camera to record one-on-one therapy with a child in a classroom or clinic. Due to stringent privacy requirements in these domains, it is imperative to protect the privacy of other individuals in the same environment. To tackle this challenge, we introduce a new visual privacy paradigm called privacy bubble. Privacy bubble is a virtual zone centered around the camera for observation whereas the rest of the environment and people are obfuscated. Most existing visual privacy systems rely on visual classifiers to identify sensitive information such as faces or bodies for protection. Any misclassification can defeat the entire purpose of privacy protection. Privacy bubble, on the other hand, relies on depth estimation to determine the extent of privacy protection. In this paper, we construct a wearable stereo-camera for depth estimation on the Raspberry Pi platform. We also propose a novel framework to quantify the uncertainty in depth measurement so as to minimize a statistical privacy risk in constructing the depth-based privacy bubble. The effectiveness of the proposed scheme is demonstrated with preliminary experimental results.

- **A surveillance framework for the protection of remote energy facilities using a hybrid multi-class object classification method** (Demo)
  Georgios Matzoulas (Centre for Research and Technology, Greece), Christos Palaskas (Centre for Research and Technology, Greece), Savvas Rogotis (Centre for Research and Technology, Greece), Dimosthenis Ioanidis (Centre for Research and Technology, Greece) and Dimitrios Tzovaras (Centre for Research and Technology, Greece)

  The proposed work addresses the need for improving the surveillance performance of existing techniques by utilizing emerging privacy-preserving mechanisms with emphasis on infrastructure protection, such as PV parks. It aims to demonstrate the potential of an algorithm that classifies moving objects extracted from low resolution infrared images, through its implementation on several typical scenarios via an integrated software application. The use of IR cameras ensures the nonobtrusive nature of surveillance. The algorithm makes use of shape descriptors along with texture features to classify the moving objects into 4 classes, human, vehicle, motorcycle and animal. It proposes an automatic way to decide when textural features are fit to be used, based on the amount of the textural information of the object. This new multi-class object classification approach also introduces the use of confidence values and a voting system to achieve a more accurate selection of the appropriate class by the classifier. The performance of the algorithm is demonstrated by its application on several scenarios, covering a wide range of experimental conditions, including four different weather conditions, two different image resolution setups and different scenario concepts, varying from simple to more complex ones, involving many classes at the same time. The demonstration results show that the algorithm performs adequately well in most of the cases, stressing the great potential of the proposed classification approach in the field of thermal imaging.

- **Cell-ID Meter App: a Tester for Coverage Maps Localization Proofs in Forensic Investigations** (Ongoing Work)
  Igor Bisio (University of Genoa, Italy), Giulio Luzzati (University of Genoa, Italy) and Andrea Sciarrone (University of Genoa, Italy)

  Even if Cell-ID based localization for mobile phones is well-known to be unreliable, it represents a method often used in forensic investigation because it is applicable “a posteriori” starting from the Call Details Records (CDRs) where the cell-ids of the Radio Base Stations (RBSs) employed by a mobile phone are archived. In general, this kind of proof cannot be easily challenged but thanks to the great expansion of smartphones and the development of their capabilities, a tester to verify the reliability of the Cell-ID localization proof can be implemented. It has been realized as smartphone App and its employment may support for more fair judgements. This paper describes the aforementioned tool and briefly reports some interesting evidences, from trials brought in the area of the City of Genoa, about the limited reliability of Cell-ID based localization proofs.

- **Feature-level Multimodal Biometric Authentication in Consumer Mobile Devices** (Demo)
  Mikhail I. Gofman (California State University, USA), Sinjini Mitra (California State University, USA), Kevin Cheng (California State University, USA) and Nicholas Smith (California State University, USA)

  Biometrics are gradually replacing passwords in consumer-level mobile devices. Though arguably more secure than passwords, mobile biometrics are vulnerable, as thieves are learning to fabricate human traits. Also, current mobile biometric systems are criticized for failing to recognize legitimate users [1]. In this paper, we show that the security and accuracy of biometric-based authentication in these devices can be improved through "multimodal" biometrics—identifying people based on multiple biometric traits. We present a novel mobile multimodal authentication method based on fusing face and voice biometrics at the feature level. We implemented our scheme on a Samsung Galaxy S5 phone and evaluated its performance using our own multimodal mobile database and the publicly available MOBIO database. Our preliminary experiments show that the scheme improves authentication accuracy by up to 2% compared to the unimodal case, and executes almost instantaneously. These results are promising; we are working toward further improvements.

- **Efficient Privacy Protection in Video Surveillance by StegoScrambling** (Demo)
  Natacha Ruchaud (Eurecom, France) and Jean Luc Dugelay (Eurecom, France)

  This paper introduces a near-lossless reversible system. It replaces sensitive RoIs (Regions of Interests) by their edges in order to protect privacy of people. Besides, the visual quality needed for security in real time is kept. The proposed system outperforms the state-of-the-art methods according to four criteria: near-lossless reversible, computation speed, usability and privacy protection. We prove the effectiveness of the proposed filter using face recognition algorithms on different images.

- **On Going Work: Group Testing for Nearest Neighbor Search with Privacy** (Ongoing Work)
  Laurent Amsaleg (Inria France), Teddy Furon (Inria France), Ahmet Iscen (Inria France) and Li Weng (Inria France)

  This paper describes an on going work where group testing helps in enforcing security and privacy in nearest neighbor search. We detail a particular scheme based on embedding and group testing. Whereas the selected embedding poorly protects the data, the group testing approach is very beneficial from a security and complexity point of view. Even when the secret parameters are disclosed, curious server or user cannot accurately recover the data.

- **Towards a self-recovery scheme for audio restoration** (Ongoing Work)
  Alejandra Menendez-Ortiz (INAOE, Mexico), Claudia Feregrino-Uribe (INAOE, Mexico), Jose Juan Garcia-Hernandezy (CINVESTAV, Mexico) and Z. Jezabel Guzman-Zavaleta (INAOE, Mexico)

  Self-recovery schemes have been proposed to restore the tampered regions of the signals they deal with, which are images and videos; however there only are fragile watermarking schemes for audio, intended to authenticate the contents or to localize tampering, but self-recovery for audio is still an open problem. This work presents two strategies devised to propose a functional self-recovery scheme for audio. One is an improvement of an existing self-recovery scheme for images and uses a Difference Expansion (DE) technique for embedding, the other is a modification that uses an Interpolation-Error Expansion (IEE) technique for embedding. Results obtained with these strategies are promising with regard to the quality of the restored signals, although more efforts have to be done in order to reduce the perceptual impact of the scheme.

- **Towards Echo Cancellation With Minimum Error For Robust Reversible Watermarking** (Ongoing Work)
  Alejandra Menendez-Ortiz (INAOE, Mexico), Claudia Feregrino-Uribe (INAOE, Mexico), Jose Juan Garcia-Hernandezy (CINVESTAV, Mexico) and Z. Jezabel Guzman-Zavaleta (INAOE, Mexico)

  Robust reversible watermarking schemes (RWS) allow the reconstruction of a host signal and the extraction of a watermark if no attacks occur, but in the presence of attacks they either: extract the watermark, or reconstruct the host signal. However, there are audio applications that require a robust RWS that can extract the watermark and reconstruct the host audio even when echo-addition attacks occur, e.g. in an annotations scenario. This document presents an echo cancellation method designed for the robust RWS scenario, it can cancel the echo from an attacked signal without using any reference signals or additional information. This echo cancellation
  method uses the cepstrum representation of the echo signals to calculate the parameters originally used in the additive echo to inverse its effects. Experimental results show that the average ODG values of 50 echo-less signals is 0.014, which means that although these reconstructed versions contain artifacts, they are inaudible. Future efforts are oriented towards a perfect echo cancellation strategy, it will be implemented as part of a RWS for audio with watermark and host robustness.

- **Video Recapture Identification by Interframe Correlation Analysis** (Ongoing Work)
  Ernesto Aparicio-Diaz (INAOE, Mexico), Claudia Feregrino-Uribey (INAOE, Mexico), and Alejandra Menendez-Ortiz (INAOE, Mexico)

  In this work a new approach to video recapture identification is presented, based on the correlation level between consecutive frames of video sequences. The proposed method defines an interframe correlation vector, calculated from the video, as a 2D representation of it. To characterize the video, statistical measures such as standard deviation are taken from the correlation vector. The statistical measures extracted from the video are compared with a trained model which uses those measures as attributes. Experimental results show that this method is suitable in the classification of recaptured videos.

- **Macro-social threats connected with anonymity: Ukrainian experience** (Ongoing Work)
  Alexander Kosenkov (Information Society Research Center, Ukraine)

  This research is dedicated to threat of social manipulations possible due to anonymity on the Internet. As basic case Ukrainian case of such manipulations is considered. The main goal of the research is to offer alternative mechanisms which could help to remove the social manipulations threat and preserve right for the anonymity on the Internet.

- **A Forensic Cloud Environment to address the Big Data challenge in Digital Forensics** (Ongoing Work)
  Oteg Tabona (University of South Wales, UK) and Andrew Blyth (University of South Wales, UK)

  We are living in a data world where most activities are expressed digitally. More and more data is generated at an exponential rate like never before in history. The phenomenal growth of data is referred to as Big Data, one of the core drivers of Big Data is technological advancements. As the technology landscape continues to advance and become popular, the number of crimes committed in the digital domains are also increasing. These trends have significantly affected digital forensics as current forensic tools cannot scale to the demand, therefore there is an urgent need of a scalable forensic tool that will tackle the Big Data challenge in Digital Forensics. This paper presents the design of a Forensic Cloud Environment that will facilitate the analysis of a forensic case involving Big Data.

17:10-18:30: **TIFS/SPL Papers Session** (Foyer)
Chair: Samson Cheung (University of Kentucky, USA)

- **A 3D Object Encryption Scheme Which Maintains Dimensional and Spatial Stability.**
  Alireza Jolfaei (Griffith University, Australia), Xin-Wen Wu (Griffith University, Australia) and Vallipuram Muthukkumarasamy (Griffith University, Australia)

  Due to widespread applications of 3D vision technology, the research into 3D object protection is primarily important. To maintain confidentiality, encryption of 3D objects is essential. However, the requirements and limitations imposed by 3D objects indicate the impropriety of conventional cryptosystems for 3D object encryption. This suggests the necessity of designing new ciphers. In addition, the study of prior works indicates that the majority of problems encountered with encrypting 3D objects are about point cloud protection, dimensional and spatial stability, and robustness against surface reconstruction attacks. To address these problems, this paper proposes a 3D object encryption scheme, based on a series of random permutations and rotations, which deform the geometry of the point cloud. Since the inverse of a permutation and a rotation matrix is its transpose, the decryption implementation is very efficient. Our statistical analyses show that within the cipher point cloud, points are randomly distributed. Furthermore, the proposed cipher leaks no information regarding the geometric structure of the plain point cloud, and is also highly sensitive to the changes of the plaintext and secret key. The theoretical and experimental analyses demonstrate the security, effectiveness, and robustness of the proposed cipher against surface reconstruction attacks.

- **First Quantization Matrix Estimation from Double Compressed JPEG Images.**
  Sebastiano Battiato (University of Catania, Italy), Giovanni Puglisi (University of Catania, Italy), Arcangelo Ranieri Bruna (University of Catania, Italy) and Fausto Galvan (University of Udine, Italy)

  One of the most common problems in the image forensics field is the reconstruction of the history of an image or a video. The data related to the characteristics of the camera that carried out the shooting, together with the reconstruction of the (possible) further processing, allow us to have some useful hints about the originality of the visual document under analysis. For example, if an image has been subjected to more than one JPEG compression, we can state that the considered image is not the exact bitstream generated by the camera at the time of shooting. It is then useful to estimate the quantization steps of the first compression, which, in case of JPEG images edited and then saved again in the same format, are no more available in the embedded metadata. In this paper, we present a novel algorithm to achieve this goal in case of double JPEG compressed images. The proposed approach copes with the case when the second quantization step is lower than the first one, exploiting the effects of successive quantizations followed by dequantizations. To improve the results of the estimation, a proper filtering strategy together with a function devoted to find the first quantization step, have been designed. Experimental results and comparisons with the state-of-the-art methods, confirm the effectiveness of the proposed approach.

- **Compressed Fingerprint Matching and Camera Identification via Random Projections.**
  Diego Valsesia (Politecnico di Torino, Italy), Giulio Coluccia (Politecnico di Torino, Italy), Tiziano Bianchi (Politecnico di Torino, Italy) and Enrico Magli (Politecnico di Torino, Italy)

  Sensor imperfections in the form of photoresponse nonuniformity (PRNU) patterns are a well-established fingerprinting technique to link pictures to the camera sensors that acquired them. The noise-like characteristics of the PRNU pattern make it a difficult object to compress, thus hindering many interesting applications that would require storage of a large number of fingerprints or transmission over a bandlimited channel for real-time camera matching. In this paper, we propose to use real-valued or binary random projections to effectively compress the fingerprints at a small cost in terms of matching accuracy. The performance of randomly projected fingerprints is analyzed from a theoretical standpoint and experimentally verified on databases of real photographs. Practical issues concerning the complexity of implementing random projections are also addressed using circulant matrices.

- **On the Use of Discriminative Cohort Score Normalization for Unconstrained Face Recognition.**
  Massimo Tistarelli (University of Sassari, Italy), Yunlian Sun (University of Sassari, Italy) and Norman Poh (University of Surrey, UK)

  Facial imaging has been largely addressed for automatic personal identification, in a variety of different environments. However, automatic face recognition becomes very challenging whenever the acquisition conditions are unconstrained. In this paper, a picture-specific cohort normalization approach, based on polynomial regression, is proposed to enhance the robustness of face matching under challenging conditions. A careful analysis is presented to better understand the actual discriminative power of a given cohort set. In particular, it is shown that the cohort polynomial regression alone conveys some discriminative information on the matching face pair, which is just marginally worse than the raw matching score. The influence of the cohort set size in the matching accuracy is also investigated. Further, tests performed on the Face Recognition Grand Challenge ver 2 database and the labeled faces in the wild database allowed to determine the relation between the quality of the cohort samples and cohort normalization performance. Experimental results obtained from the LFW data set demonstrate the effectiveness of the proposed approach to improve the recognition accuracy in unconstrained face acquisition scenarios.

- **A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion.**
  Cai Li (University of New South Wales at Canberra, Australia), Jiankun Hu (University of New South Wales at Canberra, Australia), Josef Pieprzyk (Queensland University of Technology, Australia)and Willy Susilo (University of Wollongong, Australia).

  Biometric cryptosystems provide an innovative solution for cryptographic key generation, encryption as well as biometric template protection. Besides high authentication accuracy, a good biometric cryptosystem is expected to protect biometric templates effectively, which requires that helper data does not reveal significant information about the templates. Previous works predominantly follow an appropriate entropy definition to measure the security of biometric cryptosystems. In this paper, we point out limitations of entropy-based security analysis and propose a new security analysis framework that combines information-theoretic approach with computational security. In addition, we construct a fingerprint-based multibiometric cryptosystem (MBC) using decision level fusion. Hash functions are employed in our construction to further protect each single biometric trait. The experimental results and security analysis demonstrate that the proposed MBC provides stronger security and better authentication accuracy compared with a cryptosystem based on single biometric.

- **On the Continuity of the Secrecy Capacity of Compound and Arbitrarily Varying Wiretap Channels.**
  Holger Boche (Technische Universität München, Germany), Rafael F. Schaefer (Princeton University, USA) and H. Vincent Poor (Princeton University, USA)

  The wiretap channel models secure communication of two users in the presence of a non-legitimate eavesdropper who must be kept ignorant of transmitted messages. The performance of such a system is usually characterized by its secrecy capacity determining the maximum transmission rate of secure communication. In this paper, the issue of whether the secrecy capacity is a continuous function of the system parameters or not is examined. In particular, this is done for channel uncertainty modeled via compound channels and arbitrarily varying channels, in which the legitimate users know only that the true channel realization is from a pre-specified uncertainty set. In the former model, this realization remains constant for the whole duration of transmission, while in the latter the realization varies from channel use to channel use in an unknown and arbitrary manner. These models not only capture the case of channel uncertainty, but are also suitable to model scenarios in which a malicious adversary influences or jams the legitimate transmission. The secrecy capacity of the compound wiretap channel is shown to be robust in the sense that it is a continuous function of the uncertainty set. Thus, small variations in the uncertainty set lead to small variations in secrecy capacity. On the other hand, the deterministic secrecy capacity of the arbitrarily varying wiretap channel is shown to be discontinuous in the uncertainty set meaning that small variations can lead to dramatic losses in capacity.

- **Robust Broadcasting of Common and Confidential Messages over Compound Channels: Strong Secrecy and Decoding Performance.**
  Rafael F. Schaefer (Princeton University, USA) and Holger Boche (Technische Universität München, Germany)

  The broadcast channel with confidential messages (BCC) consists of one transmitter and two receivers, where the transmitter sends a common message to both receivers and, at the same time, a confidential message to one receiver which has to be kept secret from the other one. In this paper, this communication scenario is studied for compound channels, where it is only known to the transmitter and receivers that the actual channel realization is fixed and from a prespecified set of channels. The information theoretic criterion of strong secrecy is analyzed in detail and its impact on the decoding performance of the non-legitimate receiver is characterized. In particular, it is shown that regardless of the computational capabilities and the applied decoding strategy of the non-legitimate receiver, his decoding error always tends to one. This gives a valuable signal processing implication of the strong secrecy criterion and identifies desirable properties of an optimal code design. Further, an achievable strong secrecy rate region is derived and a multiletter outer bound is given. Both together yield a multiletter expression of the strong secrecy capacity region of the compound BCC.

- **An investigation of local descriptors for biometric spoofing detection.**
  Diego Gragnaniello (University Federico II of Naples, Italy) Giovanni Poggi (University Federico II of Naples, Italy), Carlo Sansone (University Federico II of Naples, Italy) and Luisa Verdoliva (University Federico II of Naples, Italy)

  Biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. The research in this field is very active, with local descriptors, based on the analysis of microtextural features, gaining more and more popularity, because of their excellent performance and flexibility. This paper aims at assessing the potential of these descriptors for the liveness detection task in authentication systems based on various biometric traits: fingerprint, iris, and face. Besides compact descriptors based on the independent quantization of features, already considered for some liveness detection tasks, we will study promising descriptors based on the joint quantization of rich local features. The experimental analysis, conducted on publicly available data sets and in fully reproducible modality, confirms the potential of these tools for biometric applications, and points out possible lines of development toward further improvements.

- **Median Filtered Image Quality Enhancement and Anti-Forensics via Variational Deconvolution.**
  Wei Fan (Beihang University, China), Kai Wang (Grenoble Institute of Technology, France), François Cayre (Grenoble Institute of Technology, France), and Zhang Xiong (Beihang University, China),

  Median filtering enjoys its popularity as a widely adopted image denoising and smoothing tool. It is also used by anti-forensic researchers in helping disguise traces of other image processing operations, e.g., image resampling and JPEG compression. This paper proposes an image variational deconvolution framework for both quality enhancement and anti-forensics of median filtered (MF) images. The proposed optimization-based framework consists of a convolution term, a fidelity term with respect to the MF image, and a prior term. The first term is for the approximation of the median filtering process, using a convolution kernel. The second fidelity term keeps the processed image to some extent still close to the MF image, retaining some denoising or other image processing artifact hiding effects. Using the generalized Gaussian as the distribution model, the last image prior term regularizes the pixel value derivative of the obtained image so that its distribution resembles the original one. Our method can serve as an MF image quality enhancement technique, whose efficacy is validated by experiments conducted on MF images which have been previously "salt & pepper" noised. Using another parameter setting and with an additional pixel value perturbation procedure, the proposed method outperforms the state-of-the-art median filtering anti-forensics, with a better forensic undetectability against existing detectors as well as a higher visual quality of the processed image. Furthermore, the feasibility of concealing image resampling traces and JPEG blocking artifacts is demonstrated by experiments, using the proposed median filtering anti-forensic method.

Wednesday, 18 November 2015

9:00-10:40: **Special Session: Physical Layer Security** (Aula Magna)
Chair: Rafael Schafer (Princeton University, USA)

9:00- 9:20: **Authentication with a Guessing Adversary.**
Farshad Naghibi (KTH Royal Institute of Technology, Sweden), Tobias Oechtering (KTH Royal Institute of Technology, Sweden) and Mikael Skoglund (KTH Royal Institute of Technology, Sweden)

In this paper, we consider the authentication problem where a candidate measurement presented by an unidentified user is compared to a previously stored measurement of the legitimate user, the enrollment, with respect to a certain distortion criteria for authentication. An adversary wishes to impersonate the legitimate user by guessing the enrollment until the system authenticates him. For this setting, we study the minimum number of required guesses (on average) by the adversary for a successful impersonation attack and find the complete characterization of the asymptotic exponent of this metric, referred to as the deception exponent. Our result relies on the results of the Guessing problem by Arikan and Merhav. Furthermore, we extend this result to the case where the adversary may have access to additional side information correlated to the enrollment data.

9:20- 9:40: **Multicasting with Untrusted Relays: A Noncoherent Secure Network Coding Approach.**
Ta-Yuan Liu (National Tsing Hua University, Taiwan), Shih-Chun Lin (National Taiwan University of Science and Technology, Taiwan) and Y.-W. Peter Hong (National Tsing Hua University, Taiwan)

We consider the problem of multicasting information from a source to a set of receivers over a layered network with intermediate relays. However, some of the relays are untrustworthy and may be subject to eavesdropping. The source wishes to enlist their help while keeping the message secret against the eavesdropper. A noncoherent wiretap channel framework is proposed to maintain secrecy over a multicasting network that employs randomized linear network coding at the relays. The secrecy capacity of the noncoherent wiretap channel is derived with the input distribution optimized using an efficient projection-based gradient decent algorithm. The untrusted relay recruitment problem is also examined based on the derived secrecy capacity. An interesting scenario is analyzed where each potentially insecure relay is randomly eavesdropped with a certain probability. Our asymptotic analysis reveals that with enough untrusted relays, there exists a threshold on the eavesdropping probability below which all untrusted relays should be recruited.

9:40-10:00: **Robust PUF based Authentication.**

Andrea Grigorescu (Technische Universität München, Germany), Holger Boche (Technische Universität München, Germany) and Rafael Schaefer (Princeton University, USA)

Physical Unclonable Functions (PUFs) can be seen as the fingerprint of a device. PUFs are ideal objects for device authentication due to its uniqueness. In this paper, PUF based authentication is studied from an information theoretical perspective considering compound sources, which models uncertainty in the PUF knowledge and some attack classes. It is shown, that authentication is robust against source uncertainty and a special class of attacks. The privacy secrecy capacity region is derived.

10:00-10:20: **Worst-Case Secrecy Rates in MIMOME Systems under Input and State Constraints.**

Anne Wolf (Technische Universität Dresden, Germany), Eduard Jorswieck (Technische Universität Dresden, Germany) and Carsten Janda (Technische Universität Dresden, Germany)

We consider the maximization of worst-case secrecy rates for a multi-antenna wiretap channel under input constraints on the transmit covariance matrix and state constraints on the eavesdropper channel. This approach yields achievable rates (and the corresponding strategies) for a definitely secure transmission, although it is assumed that the transmitter does not have perfect information about the eavesdropper channel. We study problems with unitarily invariant constraints and show how these results can be applied to problems with more general constraints. Our results are illustrated with two detailed examples.

10:20-10:40: **Full-Duplex vs. Half-Duplex Secret-Key Generation.**

Hendrik Vogt (Ruhr University Bochum, Germany) and Aydin Sezgin (Ruhr University Bochum, Germany)

Secret-key agreement from reciprocal wireless channels has been considered a valuable supplement for security at the physical-layer (PHYSEC). On the one hand, full-duplex (FD) communication is regarded as one of the key technologies in future 5G systems. On the other hand, the success of 5G depends, among other things, on the ability to allow for secure communication. However, most key agreement models are based on half-duplex (HD) setups. Therefore, in this work, we propose representations of key generation models in both HD and FD modes. We analyze the performance of FD vs. HD modes by utilizing the key-communication function of secret-key agreement. It turns out that, for the application of key agreement, the FD approach enables advantages over the conventional HD setups. In particular, we derive a condition that guarantees improved performance of FD over HD mode in the high SNR regime.

10:40-11:10: Communication Break

11:10-12:30: Oral Session: Multimedia Forensics I (Aula Magna)
Chair: Mauro Barni (University of Siena, Italy)

11:10-11:30: **A Second Look at First Significant Digit Histogram Restoration.**
Matthias Kirchner (Binghamton University, USA) and Sujoy Chakraborty (Binghamton University, USA)

We analyze a class of first significant digit (FSD) histogram restoration techniques designed to cover up traces of previous JPEG compressions under a minimum cost constraint. We argue that such minimal distortion mappings introduce strong artifacts to the distribution of DCT coefficients, which become particularly prevalent in the domain of second significant digits (SSDs). Empirical findings from large image databases give insight into SSD distributions of DCT coefficients of natural images and demonstrate how images that underwent FSD histogram restoration deviate from natural images.

11:30-11:50: **Improved 3D Lighting Environment Estimation for Image Forgery Detection.**
Bo Peng (Institute of Automation, Chinese Academy of Sciences, China), Wei Wang (Institute of Automation, Chinese Academy of Sciences, China), Jing Dong (Institute of Automation, Chinese Academy of Sciences, China) and Tieniu Tan(Institute of Automation, Chinese Academy of Sciences, China)

3D lighting environment is an important clue in an image that can be used for image forgery detection. Existing forensic methods exploring lighting environment consistency are based on many assumptions, among which convexity and constant reflectance of the surface are two critical ones. In this paper, we propose an improved 3D lighting environment estimation method based on a more general surface reflection model. We relax the two assumptions by incorporating the local geometry and texture information into our position dependent reflection model. The proposed model is more realistic for objects like human faces which are non-convex and textured. Experiments show that the proposed method can achieve improved lighting environment estimation accuracy compared to the previous method and has better forgery detection efficacy

11:50-12:10: **General-Purpose Image Forensics Using Patch Likelihood under Image Statistical Models.**
Wei Fan (GIPSA-lab, Grenoble INP, France), Kai Wang (GIPSA-lab, Grenoble INP, France) and François Cayre (GIPSA-lab, Grenoble INP, France)

This paper proposes a new, conceptually simple and effective forensic method to address both the generality and the fine-grained tampering localization problems of image forensics. Corresponding to each kind of image operation, a rich GMM (Gaussian Mixture Model) is learned as the image statistical model for small image patches. Thereafter, the binary classification problem, whether a given image block has been previously processed, can be solved by comparing the average patch log-likelihood values calculated on overlapping image patches under different GMMs of original and processed images. With comparisons to a powerful steganalytic feature, experimental results demonstrate the efficiency of the proposed method, for multiple image operations, on whole images and small blocks.

12:10-12:30: **Image Splicing Detection based on General Perspective Constraints.**
Massimo Iuliani (University of Florence, Italy), Giovanni Fabbri (University of Florence, Italy) and Alessandro Piva (University of Florence, Italy)

Image Forensics offers numerous solutions for authenticating the contents of digital images. Unfortunately most of these technologies are ready to work only in controlled environments and their performances heavily drop when applied in real world scenario (e.g, social network, low resolution image, …) where the images have gone through a chain of unknown processes. In this paper we present a method for forgery detection based on perspective constraints; similar techniques have been proposed in the past but they are effective only when the image is captured with no tilt and no roll thus been unusable in most natural scenes. Here, this solution is extended to include these cases, and we show its applicability even when the image is exchanged through a social network (specifically Facebook and Twitter) where the image is subjected to heavy compression.

11:10-12:30: Oral Session: Biometrics II (Aula del Consiglio)
Chair: Walter Scheirer (University of Notre Dame, US)

11:10-11:30: **Integrating Rare Minutiae in Generic Fingerprint Matchers for Forensics.**
Ram P. Krish (Universidad Autonoma de Madrid, Spain), Julian Fierrez (Universidad Autonoma de Madrid, Spain) and Daniel Ramos (Universidad Autonoma de Madrid, Spain)

Automated Fingerprint Identification Systems (AFIS) are commonly used by law enforcement agencies to narrow down the possible suspects from a criminal database. AFIS do not use all discriminatory features available in fingerprints but typically use only some types of features automatically extracted by a feature extraction algorithm. Latent fingerprints obtained from crime scenes are usually partial in nature which results to only very few number of reliable minutiae compared to full fingerprints. Comparing a partial minutiae pattern to a full minutiae pattern is a difficult problem. Towards solving this challenge, we propose a method that exploits extended fingerprint features (unusual/rare minutiae) not commonly considered in typical minutiae-based matchers. The method we propose in this work can be combined with any existing minutiae-based matcher. We first compute a similarity measure based on least squares between latent and tenprint minutiae points, with rare minutia feature as reference point. Then the similarity score of the reference minutiae-based matcher at hand is modified based on the least square similarity measure. Thus, the modified similarity score also incorporates the contribution of rare minutia features. We use a realistic forensic fingerprint casework database in our experiments which contains rare minutia features obtained from Guardia Civil, the Spanish law enforcement agency. Experiments are conducted using two minutiae-based matchers as a reference, namely: NIST-Bozorth3 and VeriFinger. We report a significant improvement in the rank identification accuracies when the reference minutiae matchers are augmented with our proposed algorithm based on rare minutia features.

11:30-11:50: **The Influence of Segmentation On Individual Gait Recognition.**
Ning Jia (University of Warwick, UK), Victor Sanchez (University of Warwick, UK), Chang-Tsun Li (University of Warwick, UK) and Hassan Mansour (Mitsubishi Electric Research Laboratories, USA)

The quality of the extracted gait silhouettes can hinder the performance and practicability of gait recognition algorithms. In this paper, we analyse the influence of silhouette quality caused by segmentation disparities, and propose a feature fusion strategy to improve recognition accuracy. Specifically, we first generate a dataset containing gait silhouette with various qualities generated by different segmentation algorithms, based on the CASIA Dataset B. We then project data into an embedded subspace, and fuse gallery features of different quality levels. To this end, we propose a fusion strategy based on Least Square QR-decomposition method. We perform classification based on the Euclidean distance between fused gallery features and probe features. Evaluation results show that the proposed fusion strategy attains important improvements on recognition accuracy.

11:50-12:10: **Some Applications of Verifiable Computation to Biometric Verification.**
Julien Bringer (Morpho, France), Hervé Chabanne (Morpho, France), Firas Kraïem (Morpho, France), Roch Lescuyer (Morpho, France) and Eduardo Soria-Vazquez (Morpho, France)

Spurred by the advent of cloud computing, the domain of verifiable computations has known significant progress in recent years. Verifiable computation techniques enable a client to safely outsource its computations to a remote server. This server performs the calculations and generates a proof asserting their correctness. The client thereafter simply checks the proof to convince itself of the correctness of the output. In this paper, we study how recent advances in cryptographic techniques in this very domain can be applied to biometric verification.

12:10-12:30: **Windowed DMD as a Microtexture Descriptor for Finger Vein Counter-spoofing in Biometrics.**

Santosh Tirunagari (University of Surrey, UK), Norman Poh (University of Surrey, UK), Miroslaw Bober (University of Surrey, UK) and David Windridge (University of Surrey, UK)

Recent studies have shown that it is possible to attack a finger vein (FV) based biometric system using printed materials. In this study, we propose a novel method to detect spoofing of static finger vein images using Windowed Dynamic mode decomposition (W-DMD). This is an atemporal variant of the recently proposed Dynamic Mode Decomposition for image sequences. The proposed method achieves better results when compared to established methods such as local binary patterns (LBP), discrete wavelet transforms (DWT), histogram of gradients (HoG), and filter methods such as range-filters, standard deviation filters (STD) and entropy filters, when using SVM with a minimum intersection kernel. The overall pipeline which consists of W-DMD and SVM, proves to be efficient, and convenient to use, given the absence of additional parameter tuning requirements. The effectiveness of our methodology is demonstrated using FV-Spoofing-Attack database which is publicly available. Our test results show that W-DMD can successfully detect printed finger vein images because they contain micro-level artefacts that not only differ in quality but also in light reflection properties compared to valid/live finger vein images.

12:30-14:00: Lunch

14:00-15:00: Keynote Talk (Aula Magna)

Privacy and Security in the Genomic Era.

Jean-Pierre Hubaux (EPFL, Lausanne, Switzerland).

15:00-20:00: Social Event

20:00: Gala Dinner

Thursday, 19 November 2015

9:00-10:40: **Oral Session: Watermarking And Data Hiding** (Aula Magna)
Chair: Alessandro Piva (University of Florence, Italy)

9:00- 9:20: **Generalised tally-based decoders for traitor tracing and group testing.**
Boris Skoric (Eindhoven University of Technology, Netherlands) and Wouter de Groot (Eindhoven University of Technology, Netherlands)

We propose a new type of score function for Tardos traitor tracing codes. It is related to the recently introduced tally-based score function, but it utilizes more of the information available to the decoder. It does this by keeping track of sequences of symbols in the distributed codewords instead of looking at columns of the code matrix individually. We derive our new class of score functions from a Neyman-Pearson hypothesis test and illustrate its performance with simulation results. Finally we derive a score function for (medical) group testing applications.

9:20- 9:40: **A Population of Eagles, Horses, and Moles: Perceptual Sensitivity to Watermark Disparity Coherence.**
Hasan Sheikh Faridul (Technicolor, France) and Gwenael Doerr (Technicolor, France)

Disparity coherent watermarking has been introduced as a means to address the unique characteristics of stereoscopic visual content. This strategy has been reported to notably improve robustness performances in prior works, especially with respect to virtual view synthesis. While disparity coherence has always been conjectured to also provide better improved fidelity, it had never been properly evaluated. This perceptual study investigates the perception of three alternate watermarking strategies for stereo visual content on a population of thirty three observers. The analysis of the results reveals that there are three categories of observers and one of these categories, which amounts to nearly one third of our observers, is extremely sensitive to watermark coherence even for low-power watermarks. Moreover, the sensitivity to watermark coherence is found to be content dependent.

9:40-10:00: **Automatic Contrast Enhancement using Reversible Data Hiding.**

Suah Kim (Korea University, Korea), Rolf Lussi (ZHAW Institute of Embedded Systems, Switzerland), Xiaochao Qu (Korea University, Korea) and Hyoung Joong Kim (Korea University, Korea)

Automatic image enhancement is increasingly becoming a popular tool for the smartphone environment. The tool automatically enhances the image right after it has been stored to enhance user's experience. But, because enhancements are subjective and dependent on the image, the original image is backed up to provide a recovery option. This requirement inevitably increases the storage requirement. In order to reduce it, a novel automatic contrast enhancement based on reversible data hiding (ACERDH) is proposed. The proposed method mimics the equalization effect observed in the basic contrast enhancement technique called global histogram equalization, while providing reversibility. The experiment visually show improved contrast. Additional experiment was done to compare the embedding capacity with an another reversible data hiding based contrast enhancement technique [4]. The proposed method is fit for automation, while providing data hiding capability and removing the additional storage requirement.

10:00-10:20: **Optimum Reversible Data Hiding and Permutation Coding.**

Félix Balado (University College Dublin, Ireland)

This paper is mainly devoted to investigating the connection between binary reversible data hiding and permutation coding. We start by undertaking an approximate combinatorial analysis of the embedding capacity of reversible watermarking in the binary Hamming case, which asymptotically shows that optimum reversible watermarking must involve not only ``writing on dirty paper'', as in any blind data hiding scenario, but also writing on the dirtiest parts of the paper. The asymptotic analysis leads to the information-theoretical result given by Kalker and Willems more than a decade ago. Furthermore, the novel viewpoint of the problem suggests a near-optimum reversible watermarking algorithm for the low embedding distortion regime based on permutation coding. A practical implementation of permutation coding, previously proposed in the context of maximum-rate perfect steganography of memoryless hosts, can be used to implement the algorithm. The paper concludes with a discussion on the evaluation of the general rate-distortion bound for reversible data hiding.

10:20-10:40: **Binary fingerprinting codes - can we prove that someone is guilty?!**

Marcel Fernandez (Universitat Politecnica Catalunya, Spain), Elena Egorova (High School of Economics, Russian Federation) and Grigory Kabatiansky (Institute for Information Transmission Problems, Russian Federation)

The Identifiable Parent Property guarantees, with probability 1, the identification of at least one of the traitors by the corresponding traitor tracing schemes, or, by IPP-codes. Unfortunately, for the case of binary codes the IPP property does not hold even in the case of only two traitors. A recent work has considered a natural generalization of IPP-codes for the binary case, where the identifiable parent property should hold with probability almost 1. It has been shown that almost t-IPP codes of nonvanishing rate exist for the case $t = 2$. Surprisingly enough, collusion secure digital fingerprinting codes do not automatically possess this almost IPP property. In practice, this means that for a given forged fingerprint, say z, a user identified as guilty by the tracing algorithm can deny this claim since he will be able to present a coalition of users that can create the same z, but he does not belong to that coalition. In this paper, we study the case of t-almost IPP codes for $t > 2$.

10:40-11:10: Communication Break

11:10-12:30: Oral Session: Adversarial Detection (Aula Magna)

Chair: Teddy Furon (Inria France)

11:10-11:30: **Detection Games with a Fully Active Attacker.**

Benedetta Tondi (University of Siena, Italy), Mauro Barni (University of Siena, Italy) and Neri Merhav (Technion, Israel Institute of Technology, Israel)

We analyze a binary hypothesis testing problem in which a defender has to decide whether or not a test sequence has been drawn from a given source P_0 whereas, an attacker strives to impede the correct detection. In contrast to previous works, the adversarial setup addressed in this paper considers a fully active attacker, i.e. the attacker is active under both hypotheses. Specifically, the goal of the attacker is to distort the given sequence, no matter whether it has emerged from P_0 or not, to confuse the defender and induce a wrong decision. We formulate the defender-attacker interaction as a game and study two versions of the game, corresponding to two different setups: a Neyman-Pearson setup and a Bayesian one. By focusing on asymptotic versions of the games, we show that there exists an attacking strategy that is both dominant (i.e., optimal no matter what the defense strategy is) and universal (i.e., independent of the underlying sources) and we derive equilibrium strategies for both parties.

11:30-11:50: **Impact of Incomplete Knowledge on Scanning Strategy.**

Andrey Garnaev (Rutgers University, USA) and Wade Trappe (Rutgers University, USA)

Security is a fundamental problem facing wireless systems employing spectrum sharing, and thus scanning algorithms are used to detect malicious or illegal activity in such systems. A crucial issue in designing such algorithms is incorporating knowledge about the environment, as well as what knowledge an adversary might have, into the scanning algorithm to improve detection performance. In particular, if such knowledge is initially incomplete, it becomes desirable to adapt one's knowledge based upon the results of the scanning activities, so as to further improve detection performance. To obtain insight into this problem, we suggest a Bayesian game-theoretical model of bandwidth scanning with learning. We show that such knowledge could change the structure of the strategies employed from distributing effort among all the bands, to band sharing or even band on/off strategies and improve detection performance. Also, we have shown that a lack of information for the scanner compare to the adversary makes the scanner strategy more sensitive to the information he has.

11:50-12:10: **On the Effectiveness of Meta-Detection for Countering Oracle Attacks in Watermarking.**

Benedetta Tondi (University of Siena, Italy), Pedro Comesaña-Alfaro (University of Vigo, Spain), Fernando Pérez-González (University of Vigo, Spain) and Mauro Barni (University of Siena, Italy)

We show that smart detection is a powerful tool to combact oracle attacks in watermarking. By devising a simple metadetector that determines whether the system is subject to a threat, oracle-based adversaries can be significantly counteracted. In a recent work, we have shown that few queries are sufficient for a simple metadetector (that just measures closeness to the detection boundary) to detect an oracle attack. However, a limitation of such analysis is the assumption that all the queries correspond to either honest users or malicious ones. In this paper we address a more realistic scenario in which the metadetector does not know whether and when the watermark system is being attacked, thus allowing for a mix in which adversarial queries are interspersed with honest ones. By focusing on this more general situation, we evaluate the performance of the metadetection and derive conditions under which powerful testing is possible.

12:10-12:30: **Detection of Interest Flooding Attacks in Named Data Networking using Hypothesis Testing.**

Ngoc Tan Nguyen (Troyes University of Technology, France), Rémi Cogranne (Troyes University of Technology, France), Guillaume Doyen (Troyes University of Technology, France) and Florent Retraint (Troyes University of Technology, France)

With the rapid growth of Internet traffic, new emerging network architectures are under deployment. However, those architectures will substitute the current IP/TCP network only if they can ensure better security. Currently, the most advanced proposal for future Internet architecture is Named Data Networking (NDN). However, new computer network architectures bring new type of attacks. This paper focuses on the detection against Interest flooding - one of the most threatening attack in NDN. The statistical detection is studied within the framework of hypothesis testing. First, we address the case in which all traffic parameters are known. In this context, the optimal test is designed and its statistical performance is given. This allows to provide an upper bound on the highest detection accuracy one can expect. Then, a linear parametric model is proposed to estimate unknown parameters and to design a practical test for which the statistical performance is also provided. Numerical results show the relevance of the proposed methodology.

12:30-14:00: Lunch

14:00-15:00: Keynote Talk (Aula Magna)

Dealing with noisy data in biometrics and PUFs.
Boris Škorić (Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands).

15:00-16:40: Oral Session: Network Security And Privacy (Aula Magna)
Chair: Juan R. Troncoso (University of Vigo, Spain)

15:00-15:20: **Trust-based Sybil Nodes Detection with Robust Seed Selection and Graph Pruning on SNS.**
Shuichiro Haruta (Keio University, Japan), Kentaroh Toyoda (Keio University, Japan) and Iwao Sasase (Keio University, Japan)

On SNS (Social Networking Services), detecting Sybils is an urgent demand. The most famous approach is called ``SybilRank'' scheme where each node evenly distributes its trust value starting from honest seeds and detects Sybils based on the trust value. Furthermore, Zhang et al. proposed to avoid trust values from being distributed into Sybils by pruning suspicious relationships before SybilRank. However, we point out that the above two schemes have shortcomings that must be remedied. In the former scheme, seeds are concentrated on the specific communities and thus the trust value is not evenly distributed. Against the latter one, a sophisticated attacker can avoid graph pruning by making relationships between Sybil nodes. In this paper, we propose a robust seed selection and graph pruning scheme to detect Sybil nodes. To more evenly distribute trust value into honest nodes, we first detect communities in the SNS and select honest seeds from each detected community. And then, based on the fact that Sybils cannot make dense relationships with honest nodes, we also propose a graph pruning scheme based on the density of relationships between trusted nodes. We prune the relationships which have sparse relationships with trusted nodes and this enables robust pruning malicious relationships even if the attackers make a large number of common friends. By the computer simulation with real dataset, we show that our scheme improves the detection accuracy of both Sybil and honest nodes.

15:20-15:40: **Privacy, Efficiency & Fault Tolerance in Aggregate Computations on Massive Star Networks.**

Shantanu Rane (Palo Alto Research Center, USA), Julien Freudiger (Palo Alto Research Center, USA), Alejandro Brito (Palo Alto Research Center, USA) and Ersin Uzun (Palo Alto Research Center, USA)

We consider the challenge of performing efficient, fault-tolerant, privacy-preserving aggregate computations in a star topology, i.e., a massive number of participants connected to a single untrusted aggregator. The privacy constraints are that the participants do not discover each other's data, and the aggregator obtains the final results while remaining oblivious to each participant's individual contribution to the aggregate. In achieving these goals, previous approaches have either assumed a trusted dealer that distributes keys to the participants and the aggregator, or introduced additional parties that withhold the decryption key from the aggregator, or applied secret sharing which either requires pairwise communication amongst the participants or incurs $O(N^2)$ ciphertext overhead at the aggregator. In contrast, we develop a protocol based on Shamir secret sharing and homomorphic encryption without assuming any additional parties. We also eliminate all pairwise communication amongst the participants and still require only $O(N^{1+\varepsilon})$ overhead at the aggregator, where $\varepsilon << 1$ for massively multiparty computation scenarios. Our protocol arranges the star-connected participants into a logical hierarchy that facilitates parallelization, while allowing for user churn, i.e., a specified number of participants can go offline after providing their data, and new participants can join at a later stage of the computation.

15:40-16:00: **Private Data Aggregation with Groups for Smart Grids in a Dynamic Setting using CRT.**

Zekeriya Erkin (Delft University of Technology, Netherlands)

Computing the total consumption within a neighbourhood or of a single households in smart grids is important for billing and statistical analysis. Fine granular data used for this purpose, unfortunately, leaks too much privacy sensitive information on the inhabitants and thus raise serious concerns. In this paper, we propose a cryptographic protocol that protects the privacy sensitive measurements while it enables the utility provider to obtain the desired statistical information. Our protocols improves the state-of-the-art in three dimensions. Firstly, from a single execution of the protocol, the utility provider can obtain the total consumption of the whole neighbourhood as well as smaller groups that are created based on their features, e.g.\ schools, hospitals, etc. Secondly, to the best our knowledge, our protocol is the first one that cope with missing measurements without invoking other protocols or relying on third parties. Thirdly, our protocol relies on simple primitives that can be implemented efficiently even on limited devices, particularly on smart meters. We achieve our goal of having a simple, efficient protocol that is suitable for groups in a dynamic setting by combining the Chinese Remainder Theorem with modified homomorphic encryption. The simplicity and the capabilities of our protocol make it very promising to be deployed in practice as shown in the analysis.

16:00-16:20: **Decision Tree-based Detection of Denial of Service and Command Injection attacks on Robotic Vehicles.**

Tuan Vuong (University of Greenwich, UK), George Loukas (University of Greenwich, UK), Diane Gan (University of Greenwich, UK) and Anatolij Bezemskij (University of Greenwich, UK)

Mobile cyber-physical systems, such as automobiles, drones and robotic vehicles, are gradually becoming attractive targets for cyber attacks. This is a challenge because intrusion detection systems built for conventional computer systems tend to be unsuitable. They can be too demanding for resource-restricted cyber-physical systems or too inaccurate due to the lack of real-world data on actual attack behaviours. Here, we focus on the security of a small remote-controlled robotic vehicle. Having observed that certain types of cyber attacks against it exhibit physical impact, we have developed an intrusion detection system that takes into account not only cyber input features, such as network traffic and disk data, but also physical input features, such as speed, physical jittering and power consumption. As the system is resource-restricted, we have opted for a decision tree-based approach for generating simple detection rules, which we evaluate against denial of service and command injection attacks. We observe that the addition of physical input features can markedly reduce the false positive rate and increase the overall accuracy of the detection.

16:20-16:40: **Single Relay Selection for Secure Communication in a Cooperative System with Multiple Full-Duplex Decode-and-Forward Relays.**

Binh Nguyen (Gwangju Institute of Science and Technology, Korea) and Kiseon Kim (Gwangju Institute of Science and Technology, Korea)

This paper investigates single relay selection problem for secure communication in a cooperative system with multiple full-duplex decode-and-forward relays, in which an eavesdropper may overhear the source confidential message through relays' transmission. We propose an opportunistic relay selection scheme which selects the relay that maximizes the system secrecy capacity. We then evaluate the performance of the proposed scheme in terms of secrecy outage probability. As a comparison, we also derive the secrecy outage probability of the conventional Max-Min relay selection scheme proposed for full-duplex relaying systems without the existence of eavesdroppers. We show that our proposed scheme outperforms the conventional counterpart. Our analytic derivations are also extensively verified by Monte-Carlo simulations.

16:40-17:10: Communication Break

17:10-18:30: Oral Session: Multimedia Forensics II (Aula Magna)
Chair: Matthias Kirchner (Binghamton University, USA)

17:10-17:30: **Fragile Sensor Fingerprint Camera Identification.**
Erwin Quiring (University of Münster, Germany) and Matthias Kirchner (Binghamton University, USA)

We study digital camera identification based on sensor noise in an adversarial environment with asymmetries. We focus on fingerprint-copy attacks, where the attacker has access to JPEG images only, while the defender may leverage uncompressed images. This leads to the notion of fragile sensor fingerprints that are only available to the defender but do not survive lossy compression. Experiments with seven different cameras suggest a highly reliable detection of the attack as long as no high quality images are shared with the public.

17:30-17:50: **Forensics of High-Quality JPEG Images with Color Subsampling.**
Matthias Carnein (University of Münster, Germany), Pascal Schoettle (University of Innsbruck, Austria) and Rainer Boehme (University of Innsbruck, Austria)

Detecting prior compression is an essential task in image forensics and can be used to detect forgery in digital images. Many approaches focus on grayscale images and assume compressions with a low quality factor which often leave visible artifacts in the image. In practice, however, color images and high quality compression are much more relevant and widespread. Block convergence has been proposed to estimate the number of JPEG compressions with quality factor 100 for grayscale images and has been shown to produce accurate results. This paper extends block convergence to the more relevant case of color images where chrominance subsampling and color conversion make the estimation more complex. By observing block convergence for macro-blocks over multiple recompressions we are able to produce accurate estimates for color images. Oftentimes block convergence for color images enables similar accuracy and allows to detect more recompressions compared to grayscale images, while maintaining a good distinction between never and once compressed images.

17:50-18:10: **Camera Model Identification Framework Using an Ensemble of Demosaicing Features.**

Chen Chen (Drexel University, USA) and Matthew Stamm (Drexel University, USA)

Existing approaches to camera model identification frequently operate by building a parametric model of a camera component, then using an estimate of these model parameters to identify the source camera model. Since many components in a camera's processing pipeline are both complex and nonlinear, it is often very difficult to build these parametric models or improve their accuracy. In this paper, we propose a new framework for identifying the model of an image's source camera. Our framework builds a rich model of a camera's demosaicing algorithm inspired by Fridrich et al.'s recent work on rich models for steganalysis. We present experimental results showing that our framework can identify the correct make and model of an image's source camera with an average accuracy of 99.2%.

18:10-18:30: **Identification of pictorial materials by means of optimized multispectral reflectance image processing.**

Lucilla Pronti (Università La Sapienza, Italy), Pasquale Ferrara (University of Florence, Italy), Francesca Uccheddu (University of Florence, Italy), Anna Pelagotti (Istituto Nazionale di Ottica, Italy) and Alessandro Piva (University of Florence, Italy)

Image spectroscopy applied to paintings may allow identifying the surface materials in a non-invasive way. The proposed method aims at optimizing, and thus reducing, the number of filters employed, while still providing a robust method, achieving similar performances of traditional ones, which employing a large number of filters. Moreover, we targeted the identification of the pigments present on the outer layer independently from their thickness, the underlying background or support, the binder employed, their aging and acquisition set-up. In order to achieve this objective, a relevant number of swatches have been prepared, on different supports and with different thicknesses and binders. Spectral reflectance curves of such chemically known pictorial layers have been recorded by means of a spectrometer and a spectrophotometer. A novel Principal Component Analysis (PCA) approach has been devised to select the most relevant wavebands, i.e. those that allow the most effective discrimination among (quasi)metameric colours. Comparisons of results using the 13 filters available on the filter wheel and of a selection of only 3 filters support the idea of the simplified version investigated in this paper being a viable alternative.

List of Authors