

June 6, 2016, Bucharest, Romania

MFSec2017

2nd International Workshop on Multimedia Forensics and Security (MFSec 2017)

In Conjunction with ACM Conference on Multimedia Retrieval (ICMR) 2017

<http://mklab.iti.gr/mfsec2017/>

CALL FOR PAPERS

As worldwide Internet penetration increases, an environment has now emerged where the fields of security and forensics are faced with novel challenges, but also with new opportunities to exploit. On the one hand, the proliferation of social media has created a new ground for illegal actions and content exchange and with it the need to track such activities whilst simultaneously protecting users. On the other hand, the increased resources provided by Web platforms, including human resources through crowdsourcing, provide novel tools for security experts and analysts. Similarly with respect to multimedia forensics, Web and social media platforms create unique challenges for forensic algorithms through the large-scale dissemination of potentially tampered multimedia content of unknown origin. At the same time, however, they offer novel tools for forensic analysis, such as contextual information or media phylogenies, that would be inaccessible outside these environments.

The 2nd International Workshop on Multimedia Forensics and Security (MFSec 2017) has the explicit aim of drawing attention to these issues by focusing on multimedia forensics and security in the Web and social media. The goal of MFSec 2017 is three-fold: First, the workshop aims at presenting cutting-edge forensic and security methods aimed at Web and social media applications. Second, it aspires to bring together key individuals from the research and professional communities, from the fields of security, forensics, and multimedia analysis and retrieval, to exchange ideas and experiences and shape the directions of the field for the future. Third, the workshop intends to evaluate the level maturity of the field, identify the current strengths and weaknesses, and encourage progress towards novel solutions to the particular challenges posed by Web and social media environments.

Authors are encouraged to submit and present a short (**4-page**) paper presenting novel contributions on a topic relevant to the Workshop. Topics of interest for this workshop include, but are not limited to:

- Crime and terrorism detection from Web and social media
- Machine learning and multimedia data mining for intelligence purposes
- Early warning systems for terrorist threats using Web and social media
- Dark Web data extraction and visualization
- User privacy and information security in social media
- Image and video forgery detection in Web and social media content
- Source attribution for Web and social media content
- Contextual multimedia verification
- Multimedia forensics and counter-forensics for the Web
- Multimedia steganography for the Web
- Social computing for multimedia verification (e.g. crowdsourcing)
- Multimedia geographic localization for Web and social media content
- Near-and partial duplicate detection for multimedia verification
- Evaluation methodologies, datasets and benchmarks for multimedia forensics and security
- Platforms and applications for indexing and retrieval of terrorist-related multimedia content for Law enforcements agents
- Search and discovery of terrorist online multimedia content in surface and dark web and social media
- Multimedia authentication and encryption for Web and social media environments

Important dates:

- Deadline for paper submission: February 28, 2017
- Notification of acceptance: March 29, 2017
- Camera-Ready Papers Due: April 26, 2017
- Workshop date: June 6, 2017

Authors who submit to the Workshop are also ENCOURAGED to submit their extended versions (by the same deadline) to the Elsevier Journal of Visual Communication and Image Representation (JVCI) Special Issue on Data-driven Multimedia Forensics and Security (<http://tinyurl.com/jjs7wuw>).

Workshop Chairs:

- Markos Zampoglou (Information Technologies Institute/CERTH, Greece)
- Stefanos Vrochidis (Information Technologies Institute/CERTH, Greece)
- Anderson Rocha (Institute of Computing, University of Campinas, Unicamp, Brazil)
- Vasilis Katos (Bournemouth University, UK)

Supporting projects:

