

CALL FOR PAPERS

IEEE SIGNAL PROCESSING MAGAZINE Special Issue on Digital Forensics

We find ourselves today in a "digital world" where most information is created, captured, transmitted, stored, and processed in digital form. Although, representing information in digital form has many compelling technical and economic advantages, it has led to new issues and significant challenges when performing forensics analysis of digital evidence. There has been a slowly growing body of scientific techniques for recovering evidence from digital data. These techniques have come to be loosely coupled under the umbrella of "Digital Forensics." Digital Forensics can be defined as "The collection of scientific techniques for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events, usually of a criminal nature."

This call for papers invites tutorial articles covering all aspects of digital forensics with an emphasis on forensic methodologies and techniques that employ signal processing and information theoretic analysis. Authors with accepted proposals will be invited to write a full manuscript. Thus, focused tutorial and survey contributions are solicited from topics, including but not limited to, the following.

Scope of topics:

- Computer Forensics - File system and memory analysis. File carving.
- Media source identification - camera, printer, scanner, microphone identification.
- Differentiating synthetic and sensor media, for example camera vs. computer graphics images.
- Detecting and localizing media tampering and processing.
- Speaker recognition and analysis methods for forensics.
- Speech transcription for forensics. Analysis of deceptive speech.
- Acoustic processing for forensic analysis - e.g. acoustical gunshot analysis, accident reconstruction.
- Forensic musicology and copyright infringement detection.
- Enhancement and recognition techniques from surveillance video/images. Image matching techniques for auto- matic visual evidence extraction/recognition.
- Steganalysis - Detection of hidden data in images, audio, video. Steganalysis techniques for natural language steganography. Detection of covert channels.
- Data Mining techniques for large scale forensics.
- Privacy and social issues related to forensics.
- Anti-forensics. Robustness of media forensics methods against counter measures.
- Case studies and trend reports.

This special issue is being simultaneously published with a special issue on the same topic of the security and privacy magazine published by the computer society. The call for papers of the security and privacy magazine special issue can be seen at <http://www.computer.org/portal/site/security/>.

Submission Procedure:

Prospective authors should submit white papers to the web submission system at <http://www.ee.columbia.edu/spm/> according to the following timetable. White papers, limited to 3 single-column double-spaced pages, should summarize the motivation, the significance of the topic, a brief history, and an outline of the content. In all cases, prospective contributors should make sure to emphasize the signal processing in their submission.

Schedule (all deadlines are firm no exceptions)

White paper due:	April 7, 2008
Invitation notification:	April 30, 2008
Manuscript due:	July 15, 2008
Acceptance Notification:	October 15, 2008

Final Manuscript due: November 15, 2008
Publication date: March, 2009

Guest Editors:

Edward Delp

Purdue University
ace@ecn.purdue.edu

Nasir Memon

Polytechnic University
memon@poly.edu

Min Wu

University of Maryland
minwu@eng.umd.edu