Societies in today’s world are becoming more and more dependent on open networks such as Internet where commercial activities, business transactions and government services are realized. This has led to the fast development of new cyber threats and information security issues which are utilized by cyber criminals. Mistrust for telecommunications and computer network technologies have tremendous socio-economic impacts on global enterprises as well as individuals. Moreover, the occurrence of international frauds often requires the investigation of facts that occur across international borders. They are also often subject to different jurisdictions and legal systems. The increased complexity of the communication and networking infrastructure is making investigation of the crimes difficult. Clues of illegal digital activities are often buried in large volumes of data that is hard to inspect in order to detect crimes and collect evidence.

This poses new challenges for law enforcements and forces computer societies to utilize digital forensics to combat the growing number of cybercrimes. Forensic professionals need to be fully prepared in order to be able to provide effective evidence. To achieve these goals forensic techniques must keep pace with new technologies. That is why the field of digital forensics is becoming more and more important for law enforcement, information and network security.

This special issue presents some of the most relevant ongoing research in cyber-crime. Topics include, but are not limited to the following:

- Cyber-crime science
- Information and network security
- Network traffic analysis and modelling for cyber-crime science
- Watermarking and intellectual property theft
- Network attacks & anomalies detection and prevention
- Protocols, systems, computer and security
- Steganography/steganalysis and covert/subliminal channels
- Artificial Intelligence (AI) based or game theory techniques for cyber-crimes detection
- Security architectures
- Digital forensics
Submission Schedule

- Manuscript due:
  - July 25, 2013

Submission Instructions:

Papers must be written in English and describe original research not published or currently under review by other journals or conferences. All relevant papers submitted will go through an external review process. Besides normal submissions, selected best papers of the IWCC 2013 (International Workshop on Cyber Crime) can be submitted to this special issue. There should be at least 30% difference between the extended/revised paper and the workshop paper, and the papers will be handled as all other papers in matters of refereeing and selection. Before submission, authors should carefully read over the Instructions for Authors, which are located at jis.eurasipjournals.com/authors/instructions. Prospective authors should submit an electronic copy of their complete manuscript through the SpringerOpen submission system at jis.eurasipjournals.com/manuscript according to the submission schedule. They should choose the correct Special Issue in the “sections” box upon submitting. In addition, they should specify the manuscript as a submission to the “Special Issue on Cyber-crime: new trends, challenges and detection” in the cover letter. All submissions will undergo initial screening by the Guest Editors for fit to the theme of the Special Issue and prospects for successfully negotiating the review process. Prospective authors are strongly encouraged to contact the co-guest Editors who will be compiling the issue.

Lead Guest Editor

Wojciech Mazurczyk, Warsaw University of Technology, Poland
Email: wmazurczyk@tele.pw.edu.pl

Guest Editors

Krzysztof Szczypiorski, Warsaw University of Technology, Poland
E-mail: ksz@tele.pw.edu.pl

Yali Liu, AT&T Labs, USA
E-mail: yl9871@att.com

Hui Tian, National Huaqiao University, China
E-mail: cshitian@gmail.com