Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2009, Article ID 257131, 1 page
doi:10.1155/2009/257131

Editorial
Secure Steganography in Multimedia Content

Miroslav Goljan[1] and Andreas Westfeld[2]

[1] *Electrical and Computer Engineering, Watson School, Binghamton University, P. O. Box 6000, Binghamton, NY 13902-6000, USA*
[2] *Faculty of Computer Science and Mathematics, HTW Dresden, Institute of Systems Architecture, University of Applied Sciences, 120701 PF, 01008 Dresden, Germany*

Correspondence should be addressed to Miroslav Goljan, mgoljan@binghamton.edu

Received 15 April 2009; Accepted 15 April 2009

Steganography, known as the art of covert communication, entered digital world about ten years ago. After gaining special interest of research groups around the world, steganography and steganalysis are slowly reaching maturity. Images produced by digital cameras are typical multimedia carriers where hiding secrets has been studied deeply. They contain a large amount of randomness that is hard to distinguish from telltale signs of hidden and eventually encrypted messages.

The security requirement in steganography ultimately means that no such detection method should exist that would be able to tell carriers with hidden messages from innocent ones with a significant reliability. Introduction of every new steganographic scheme spurred a number of publications on steganalysis of that scheme. Empirically determined secure capacities shrink with advances in steganalysis. A hope for finding general optimal solutions is narrow since they have to be tied to carrier models. To achieve undetectability, steganographers minimize the impact of message data embedding on the carrier in two ways, by content-aware embedding in various transform domains and by applying advanced coding techniques. While the first is a kind of an art that needs to undergo the scrutiny of steganalysis testing and validating, the second is much more of a mathematical science. Theoretical bounds on coding efficiency are known but hard to achieve in practical schemes. Thus, secure steganographic capacity is difficult to determine for multimedia carriers and remains to be an open issue.

We are delighted to present five papers devoted to the above mentioned aspects of steganography and its counterpart, steganalysis. Fontaine and Galand prove the power of established structured codes in "How can Reed-Solomon codes improve steganographic schemes." While syndrome coding in steganographic schemes tends to reduce distortion during embedding, Miche et al. in "Reliable Steganalysis Using a Minimum Set of Samples and Features" push sensitivity of universal steganalysis a step further and reduce secure capacities of any steganography a bit. "Steganography in 3D Geometries and Images by Adjacent Bin Mapping" presented by Wu and Dugelay introduces a new countermeasure to steganography detection through histogram characteristic function.

JPEG compression format for images became the one that attracts steganographers the most. Rossi, Garzia, and Cusani return to the topic with "Peak-Shaped-Based Steganographic Technique for JPEG Images." Their novel model-based steganographic technique for JPEG images involves heuristic assumptions about the shape of the DCT frequency histograms, and finally, both aspects—coding and embedding operation—are merged in the design of a new scheme by Chao et al. described in "A Novel Image Data Hiding Scheme with Diamond Encoding."

Our thanks belong to the authors and to all reviewers for their contribution to this journal. We hope that readers will find the papers interesting at least and that blank pages in steganography area will continue being filled.

Miroslav Goljan
Andreas Westfeld