GUEST EDITORIAL

Special Section on Security, Steganography, and Watermarking

Jana Dittmann
Otto-von-Guericke-Universität Magdeburg
Institut für Technische und Betriebliche Informationssysteme
Universitätsplatz 2
39106 Magdeburg, Germany
E-mail: jana.dittmann@iti.cs.uni-magdeburg.de

Edward J. Delp
Purdue University
School of Electrical and Computer Engineering
465 Northwestern Avenue
West Lafayette, Indiana 47907-2035
E-mail: ace@ecn.purdue.edu

Motivated by the annual conference on Security, Steganography, and Watermarking of Multimedia Contents at the IS&T/SPIE Symposium on Electronic Imaging, the objective of this special section on Security, Steganography, and Watermarking is to present key issues in the areas of data authentication and data manipulation recognition, user authentication, detection of hidden communication channels as well as trade-offs for robust digital watermarking and watermarking benchmarking approaches. We expect the special section to motivate these research fields and show the most relevant problems and actual solutions.

The special section consists of six reviewed papers. The papers address theoretical and practical issues with a high degree of innovation as well as interesting improvements of existing art or new ideas and research directions.

The first paper, "Image manipulation detection" by Bayram, Avcibaş, Sankur, and Memon, discusses emerging technologies in the digital data authentication field by presenting techniques and methodologies for validating the authenticity of digital images and testing for the presence of doctoring and manipulation operations. Three categories of forensic features are reviewed and the design of classifiers between doctored and original images is discussed. The three categories of features are the binary similarity measures between the bit planes, the image quality metrics applied to denoised image residuals, and the statistical features obtained from the wavelet decomposition of an image. The performance of classifiers with respect to selected controlled manipulations as well as to uncontrolled manipulations is analyzed. The tools for image manipulation detection are treated under feature fusion and decision fusion scenarios. The three forensic features were tested against the background of single manipulations and multiple manipulations, as would actually occur in doctoring images. The set of single-manipulation experiments shows that it is best to select features from the general pool of all categories (feature fusion). In the second set of experiments with multiple manipulations, the best strategy was to use different types of classifiers (experts), one per manipulation, and then fuse their decisions.

Besides data authentication challenges, user authentication applications, especially biometric user authentication applications, are stepping into a new dimension with respect to the size and complexity, due to the decision of many countries to introduce biometric travel documents. Along with this development, many problems have become increasingly relevant. The second paper, "Handwriting biometrics: issues of integration in identification documents and sensor interoperability" by Vielhauer, addresses two of these problems: security and privacy-preserving storage of biometric references and issues of sensor interoperability. For the first problem, security aspects of storage methods based on physical components, digital image processing, and centralized data storage techniques are discussed and reviewed. Key research problems with the biggest impact on specified deficiencies in the field of secure physical storage in embedded devices are summarized. For the second problem, an intersensor evaluation methodology using the example of handwriting is introduced and extended by a new verification algorithm called BioHash. The concept is experimentally cross-validated and main conclusions are drawn. For example, the degradation of recognition accuracy in online signature verification may reach up to a factor of 4.4 for nonskilled forgeries, when cross-sensor verification is involved. Alternative semantic classes such as individual symbols show a similar tendency, although the absolute degradation factor appears to be lower. Semantic alternatives to signatures such as pass phrases or hand-drawn symbols have been shown to be well suited for online handwriting biometrics.

The third paper, "Performance study of common image steganography and steganalysis techniques" by Kharrazi, Sencar, and Memon, investigates the performance of state-of-the-art universal steganalyzers proposed in the literature. The paper presents comprehensive test results of these universal steganalyzers with a number of well-known steganographic embedding techniques working in the spatial and transform domains as well as with a large dataset of JPEG images, obtained by randomly crawling a set of publicly available websites and classified into image properties such as size, quality, and texture. The steganalyzer performance is presented within a comparative evaluation and undetectability results are obtained at various embedding rates (message length). The overall results indicate that the performance of steganalysis techniques is affected by the JPEG quality factor and JPEG recompression artifacts serve as a source of confusion for almost all steganalysis techniques.

The fourth paper, "Watermark recovery from 2-D views of a 3-D object using texture or silhouette information" by Bennour, Garcia, and Dugelay, describes a novel framework for watermarking 3-D objects using their texture or silhouette information. It is an extraordinary approach for watermarking 3-D objects and retrieving the mark from resulting 2-D images or videos having used the 3-D synthetic object, thus protecting the visual representations of the object. This is an important issue since it is usually more frequent to locate and recover suspect represented 2-D views of a 3-D object than the 3-D object itself.

In the fifth paper, "Watermark evaluation testbed" by Guitart, Kim, and Delp, the reader finds a contribution to the role and the design of benchmarking in digital watermarking to provide a fair and automated evaluation service. The paper presents a software-engineering-driven discussion of watermarking benchmarking system design and the goal is to introduce a web-based digital image watermark evaluation system known as the watermark evaluation testbed (WET). WET consists of reference software that includes both watermark embedders and detectors, attacks, evaluation modules, and a large image database. The authors show WET as a platform where any watermarking researcher can test not only the performance of known techniques, but also their own techniques. The proposed benchmarking system tries to overcome gaps mainly known from existing benchmarks: (a) design for any kind of user, from beginners to watermarking experts; (b) user involvement in the whole process of testing a watermarking technique by offering several tools such as a large image database, implemented well-known watermarking techniques, and various evaluation tools; and (c) individual proposal and testing procedures by uploading new attack and evaluation functions to the benchmark system and comparisons to other ones of the same type.

Finally, in the sixth paper entitled "Reliability engineering approach to digital watermark evaluation," Kim and Delp present an extended framework by applying reliability testing to robust still-image watermark evaluation. In reliability testing, a system is evaluated in terms of quality, load, capacity, and performance in accordance to a specified fidelity requirement under a given set of attacks and images. The authors introduce a quality measure that corresponds to image fidelity. A conditional mean of pixel values is used to compensate for volumetric attacks such as gamma correction and histogram equalization. To compensate for geometrical attacks, error concealment and perfect motion estimation assumption is introduced. The capacity is defined as the minimum embedding strength parameter and the maximum data payload that meet specified error criteria. Load is then defined to be the actual embedding strength and data payload of a watermark. The performance is measured with the bit error rate and with the receiver operating characteristics of a watermarking algorithm for different attacks and images. Evaluation results of three robust watermarking paradigms for various loads, attacks, and images are presented and discussed.

Jana Dittmann studied computer science and economy at the Technical University in Darmstadt. In 1999, she received her PhD from the Technical University of Darmstadt. She has been a full professor in the field of multimedia and security at the Otto-von-Guericke-University Magdeburg since September 2002. she specializes in the field of multimedia security. Her research is mainly focused on security aspects in the field of digital watermarking, content-based digital signatures, and biometrics for data and user authentication as well as for copyright protection. She has many national and international publications, is a member of several conference program committees, and organizes workshops and conferences in the field of multimedia and security issues. She is an associate editor for the *Multimedia Systems Journal*, the *Journal of Electronic Imaging*, and the *IEEE Transactions on Information Forensics and Security*. Dr. Dittmann is a member of the Association for Computing Machinery and the Gesellschaft für Informatik.

Edward J. Delp received BSEE (cum laude) and MS degrees from the University of Cincinnati, and a PhD degree from Purdue University. In May 2002 he received an Honorary Doctor of Technology from the Tampere University of Technology in Tampere, Finland. From 1980 to 1984, Dr. Delp was with the Department of Electrical and Computer Engineering, University of Michigan, Ann Arbor, Michigan. Since August 1984, he has been with the School of Electrical and Computer Engineering and the Department of Biomedical Engineering at Purdue University, West Lafayette, Indiana. In 2002 he received a chaired professorship and currently is The Silicon Valley Professor of Electrical and Computer Engineering and Professor of Biomedical Engineering. His research interests include image and video compression, multimedia security, medical imaging, multimedia systems, and communication and information theory. Dr. Delp has also consulted for various companies and government agencies in the areas of signal, image, and video processing, pattern recognition, and secure communications. He has published and presented more than 280 papers. Dr. Delp is a Fellow of the IEEE, a Fellow of the SPIE, a Fellow of the Society for Imaging Science and Technology (IS&T), and a Fellow of the American Institute of Medical and Biological Engineering. In 2004 he received the Technical Achievement Award from the IEEE Signal Processing Society for his work in image and video compression and multimedia security. He is a member of Tau Beta Pi, Eta Kappa Nu, Phi Kappa Phi, Sigma Xi, and the Association for Computing Machinery. Dr. Delp is a registered professional engineer.