EURASIP Journal on Applied Signal Processing 2002:2, 123–125


# Editorial

**Mauro Barni**
*Department of Information Engineering, University of Siena, Via Roma 56, 53100-Siena, Italy*
*Email: barni@dii.unisi.it*

**Franco Bartolini**
*Department of Electronics and Telecommunications, University of Florence, Via S. Marta 3, 50139-Firenze, Italy*
*Email: barto@lci.det.unifi.it*

**Jessica Fridrich**
*Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY 13902, USA*
*Email: fridrich@binghamton.edu*

The field of data hiding in the context of digital technology is quite young. Although the first paper on electronic data embedding can be traced back to a patent application issued in 1954, the active research in this field began only in the early nineties. The following years have witnessed an exponential increase in the volume of published articles and patents. By now, steganography and digital watermarking have been established as stand-alone fields with their dedicated regular international gatherings.

The first applications, that have driven the research effort in the early beginnings, focused on copyright protection of multimedia data exchanged in digital form. Research was mainly oriented towards robust watermarking, that is, the insertion within to-be-protected digital product of an imperceptible code bearing some information about the product itself, that is, the product owner, its allowed uses, or the buyer's ID for tracing purposes. These applications have spawned a plethora of problems ranging from secure protocols, design of supporting infrastructure, to an intense research on security and development of attacks.

As the research continued, it has become evident that many other application scenarios exist where data hiding could be applied successfully. Fragile watermarks were proposed for detection of malicious and inadvertent manipulations and for authentication purposes. Steganography, or covert communication, saw the first attempts to formalize the concept of steganographic security and prove strengths as well as weaknesses of proposed supposedly secure covert schemes. Other commercial applications, such as broadcast monitoring, digital cinema, image and video captioning, audio-in-video embedding for multilanguage broadcasting, image and video indexing, transmission error recovery and concealment, and others have generated rapidly increasing interest among industrial and academic researchers.

The field of data hiding has also certain special appeal so typical of every newly emerging area—it is pristine and largely unexplored. If the applications and concepts could be compared to apple trees and the problems to their fruits, one could say that there are still a number of trees that were not visited bearing large, juicy apples, with a few pieces hanging quite low. Some trees have been visited so many times that one needs a long ladder to get to new fruits. The goal of this special issue is to reveal the existence of new trees or as yet unvisited branches of existing trees, presenting to you the fruit—new results and insights, thus paving the way for future developments in the field and for a better understanding of its potential in today's world.

The special issue starts with a review on the history, present, and future of applications of data hiding written by Cox and Miller. The authors ask provocative questions about the future fate of data hiding while giving examples of practical applications. In their view, the application that gave birth to the recent research activity—the copyright protection—is giving way to other technologies, such as broadcast monitoring, authentication, and tracking content distributed within corporations. According to Cox and Miller, while considerable progress has been made toward enabling these applications—perceptual modeling, security threats and countermeasures, and the development of a bag of tricks for efficient implementations—further progress is needed in methods for handling geometric and temporal distortions. The paper has a very extensive bibliography, which

could be used as a starting point for those just entering the field.

Sharma and Decker present a highly original application of data hiding, in which a traditional analog media or object is connected to the digital world using an embedded digital watermark. In this way, the value of the analog media can be greatly enhanced since a number of possible applications usually confined to the digital world are enabled. More specifically, the authors present the Smart Toy concept, where digital watermarking is used to augment the play value of ordinary toys. The watermark transforms the toy into an extraordinary object, which is connected to a digital entity (such as a computer or the Internet). Upon detecting the watermark, which amounts to recognizing the object, the digital entity can invoke a multitude of responses.

Hilton gives a note on watermark development from the commercial context. The article is an interesting, sharply opinioned essay. Hilton calls for more academic research motivated by practical problems. Many may find Hilton's article provocative in its style, which is why we, editors, believe it has its place in this special issue simply because it will stir discussions and will help shape explorations in academia. The editors share the belief that pure theoretic academic research that is free of the application burden and industrial research motivated by practical problems form a delicate symbiosis that should be carefully nurtured.

In the next paper, Wu presents a very ingenious way for image authentication via halftoning and coordinate projection. His method belongs to the class of self-embedding methods in which the image, or its approximation, is embedded in itself. Localized manipulation, such as feature adding and removal can be not only detected but also at least partially "undone" by recovering the original features from the embedded data. Thus, self-embedding makes digital images capable of repairing themselves after inadvertent or malicious distortion. The method described by Wu provides an astonishingly simple and elegant solution to this problem for halftoned images.

Robust data hiding and lossy compression are in a strict antagonistic relationship. Watermark needs to be hidden in those parts of the image that are not removed or significantly modified by the compression algorithm. On the other hand, the existence of such a gap may prompt researchers toward new, better compression designs. Campisi and his co-authors decided to combine those two seemingly conflicting areas. They robustly embed the color information in the image to obtain a higher quality compression algorithm for color images. This unconventional approach provides surprisingly better results when compared to existing wavelet compression schemes for color images.

Robie and Mersereau describe an innovative application for video error correction using steganography. The transmission of any data is always subject to corruption due to errors, but video transmission, because of its real time nature must deal with these errors without retransmission of the corrupted data. The authors show how these errors can be handled using forward error correction in the encoder or error concealment techniques in the decoder. Their MPEG-2 compliant codec uses data hiding to transmit error correction information and several error concealment techniques in the decoder. The decoder resynchronizes more quickly with fewer errors than traditional resynchronization techniques. It also allows for perfect recovery of differentially encoded DCT-DC components and motion vectors. This provides for a much higher quality picture in an error-prone environment while creating an almost imperceptible degradation of the picture in an error-free environment.

Steinebach et al. describe how digital watermarks can be used to enable innovative e-commerce and m-commerce strategies. More specifically, the introduction of a digital watermark within a media is seen as a new way to provide transparent access-control mechanisms. Several possible application scenarios are described in the paper, including, just to mention some, "Try&Buy" mechanisms to general means for long-term customer relationships, advertisement, bonus programs. Watermarking methods to be used for establishing services in a secure way for conditional access services based on digital watermarking combined with cryptographic techniques, are discussed as well.

Almost all previously proposed data hiding techniques for images and other digital products are lossy in the sense that some part of the image is irreversibly replaced with the data. In their paper, Fridrich et al. introduce a new paradigm in data hiding—lossless embedding. The lossless techniques enable embedding data in such a way that it is possible to recover the original image after the embedded data is extracted. Thus, there is no loss of quality of the image due to embedding. This very unique and novel concept is elaborated for both raw, uncompressed formats and lossy formats (JPEG). It is shown how the lossless embedding can be used for the construction of novel fragile authentication watermarks and for the development of extremely accurate and sensitive methods for detection of hidden data. Lossless embedding is especially useful in cases when embedding distortion is not acceptable due to legal reasons (i.e., for medical images or forensic images used in the court as evidence) or due to unusual viewing conditions, such as military images scrutinized after enhancement and under extreme zoom.

The last paper of this issue, by Bartolini et al., deals with robust watermarking of cartographic images. The field of robust watermarking has long been plagued with the problem of how to recover the watermark from an image that has undergone a combined operation of cropping, change of scale, rotation, and shift. Bartolini et al. show that at least for a special class of images—maps and cartographic images—the solution can be quite simple, robust, and elegant. They use the text commonly present in cartographic images for geometrical normalization of the image before watermark embedding and extraction. There are at least two major advantages of this approach that make it suitable for practical use: the technique can be combined with any watermarking method and it removes the need for embedding special registration patterns thus minimizing the embedding distortion.

As our final note, we want to express our thanks to all contributing authors for their effort in helping to make this

special issue a reality. The papers will hopefully show new paths and give a new sense of direction to everybody working in this new exciting field of data hiding.

*Mauro Barni*
*Franco Bartolini*
*Jessica Fridrich*

**Mauro Barni** was born in Prato, Italy, in 1965. He graduated in electronic engineering at the University of Florence in 1991. He received the Ph.D. in informatics and telecommunications in October 1995. From 1991 through 1998 he was with the Department of Electronic Engineering, University of Florence, Italy, where he worked as a postdoc researcher. Since September 1998, he has been with the Department of Information Engineering, of the University of Siena, Italy, where he works as Assistant Professor. His main interests are in the field of digital image processing and computer vision. His research activity is focused on the application of image processing techniques to copyright protection and authentication of multimedia data (digital watermarking), and to the transmission of image and video signals in error-prone, wireless, environments. He is author/co-author of more than 100 papers published in international journals and conference proceedings. Mauro Barni is a member of the IEEE, where he serves as member of the Multimedia Signal Processing Technical Committee (MMSP-TC).

**Franco Bartolini** was born in Rome, Italy, in 1965. In 1991, he graduated (cum laude) in electronic engineering from the University of Florence, Florence, Italy. In November 1996, he received the Ph.D. degree in informatics and telecommunications from the University of Florence. Since November 2001, he is Assistant Professor at the University of Florence. His research interests include digital image sequence processing, still and moving image compression, nonlinear filtering techniques, image protection and authentication (watermarking), image processing applications for the cultural heritage field; signal compression by neural networks, and secure communication protocols. He has published more than 100 papers on these topics in international journals and conferences. He holds two Italian patents in the field of digital watermarking. Dr. Bartolini is a member of IEEE and IAPR.

**Jessica Fridrich** is a research professor at the Center for Intelligent Systems at the State University of New York, Binghamton. In 1987, she received her M.S. degree in applied mathematics from Czech Technical University in Prague, Czech Republic, and her Ph.D. in systems science in 1995 from the State University of New York in Binghamton. Her main research interests are in the field of steganography and steganalysis, digital watermarking, authentication and tamper detection, and forensic analysis of digital images. In the last six years, Fridrich's research has been steadily supported by the US Air Force in the form of 13 research grants total worth over US$1.3million, generating five US and international patents.