Preface

Digital media, like audio, video, images, and other multimedia documents, can be protected against copyright infringements with invisible, integrated patterns. Such methods are based on steganography and digital watermarking techniques. Most watermarks are inserted as a plain-bit or adjusted digital signal using a key-based embedding algorithm. The embedded information is hidden (in low-value bits or least significant bits of picture pixels, frequency, or other value domains) and linked inseparably with the source data structure. For the optimal watermarking application a trade-off between competing criteria such as robustness, non-perceptibility, non-detectability, and security have to be made. Most watermarking algorithms are not resistant to all attacks and even friendly attacks such as file and data modifications can easily destroy the watermark.

The features of the digital world lead to economical chances such as cheap distribution and also to serious risks in simplifying unauthorized copying and distribution (Rosenblatt, Trippe, & Mooney, 2002). In order to solve intellectual property problems of the digital age, two basic procedures are used: "buy and drop," linked to the destruction of various peer-to-peer solutions and "subpoena and fear," as the creation of non-natural social fear by specific legislations. Although customers around the world are willing to buy digital products over networks, the industry is still using conventional procedures to push such a decisive customer impulse back into existing and conventional markets.

The importance and the supposed economical thread for copyright holders are clarified by initiatives of the entertainment industry, such as VIVA (Visual Identity Verification Auditor) (VIVA, n.d.) and SDMI (Secure Digital Music Initiative) (SDMI, n.d.). Although distributors and artists already recognize the advantages in making their material available online, they will not go further into the online business until their content can be protected by technical and wide law regulations. As new intellectual property changes became new European law in 2003 and begin to fit the proposals of the World Intellectual Property Organi-

zation (WIPO), political signals, which prove their importance, were set. Therefore, the features of the digital world lead to economical chances as well as to serious problems in simplifying unauthorized copying and distribution. Digital watermarking is a possibility to interface and close the gap between copyrights and digital distribution.

This book will take the reader through a series of discussions that describe, analyze, explain, and hypothesize about digital watermarking technology and its usage.

In Chapter I, *Digital Watermarking: An Introduction*, Tino Jahnke and I give an overview on the methodology of digital watermarking, as well as on requirements of applications, applications, and a categorization of attacks on digital watermarks. There is also a short summary of the historical development of digital watermarking technology. Activities, initiatives, and projects of different associations and interest groups are discussed.

The main focus of Chapter II, *Digital Watermarking Schemes for Multimedia Authentication*, written by Chang-Tsun Li, is on multimedia data authentication. The technical aspects of security, resolution of tamper localization, and embedding distortion are explained. Fragile, semi-fragile, and reversible schemes are the three main categories of watermarking approaches to the issues and challenges that are presented. Merits and limitations of the specific schemes are compared and discussed.

Dan Yu and Farook Sattar focus in Chapter III, *Digital Watermarking for Multimedia Transaction Tracking,* on the issue of transaction tracking in multimedia distribution applications through digital watermarking technology. An approach is proposed that can overcome the problems of existing watermarking schemes. In the absence of the original data, watermark, embedding locations, and strengths, the watermarking scheme is introduced for efficient watermark extraction with some side information. The robustness of the proposed scheme is discussed.

In Chapter IV, *A New Public-Key Algorithm for Watermarking of Digital Images*, Eberhard Stickel presents a two-dimensional public-key algorithm that is based on a one-time digital signature scheme in non-abelian groups. The public key is certified by a trusted third party. Authenticity may be verified by anybody who knows the certified public key. The approach is discussed in relation to images made by surveillance cameras of automatic teller machines (ATMs) in financial institutions.

Zhang Li and Sam Kwong present in Chapter V, *Geometric Distortions Correction Using Image Moment in Image Watermarking,* a method for detecting and recovering geometrical attacks, such as rotation, scaling, and translation, by using geometric moments of the original image. The moment information can be used as a preprocess of the extraction process. Different types of watermarking techniques are analyzed.

The main focus of Chapter VI, *Audio Watermarking: Requirements, Algorithms, and Benchmarking*, by Nedeljko Cvejic and Tapio Seppänen, is on the usage of digital watermarking for audio data. Audio watermarking algorithms are characterized. Signal modifications that are usually used to distort embedded watermarks and to prevent detection of hidden data are presented. Recently developed and future applications areas are listed.

Jong-Nam Kim and Byung-Ha Ahn introduce in Chapter VII, *MPEG Standards and Watermarking Technologies,* watermarking technologies of MPEG standards. A framework of watermarking technology for intellectual property protection is presented as well as an overview of MPEG-2/4, IPMP standard of MPEG-2/4, and watermarking technologies of MPEG-2/4 IPMP. The concept of IPMP and required technical items are summarized. MPEG-21 and its part 11, PAT (Persistent Association Technologies) methodologies, requirements, and evaluation methods are described. Future trends of MPEG-related watermarking technologies and requirements are discussed.

Ernst Leiss outlines in Chapter VIII, *Time-Variant Watermarks for Digital Videos: An MPEG-Based Approach,* an approach that permits a significant increase of the amount of information that can be accommodated in a watermark. The approach is formulated assuming the video is represented in an MPEG format. Implementation issues of time-variant watermarks are discussed with emphasis on defeating attacks using filtering, cropping, resizing, and other standard methods used to defeat watermarks, such as changing existing frames, as well as new attacks, such as removing, repeating, or permuting frames.

Finally, Alexander P. Pons and Hassan Aljifri present in Chapter IX, *Active Watermarking System: Protection of Digital Media,* a novel approach that combines the reactive rule-based scheme of an active database management system with the technology of digital watermarking to automatically protect digital data. The integration of these two technologies provides a powerful mechanism for protecting digital data in a consistent and formal manner.

References

Rosenblatt, B., Trippe, B., & Mooney, S. (2002). *Digital rights management—Business and technology*. New York: M&T Books.

SDMI. (n.d.). Retrieved June 4, 2004, from *http://www.sdmi.org*

VIVA. (n.d.). Retrieved June 4, 2004, from *http://www.intec.rug.ac.be/Research/Groups/hfhsdesign/viva/*