Preface

The digital information revolution has brought about profound changes in our society and our lives. New devices and powerful software have made it possible for consumers worldwide to create, manipulate, share, and enjoy the multimedia data. Internet and wireless networks offer ubiquitous channels to deliver and to exchange multimedia information for such purposes as remote collaboration, distant learning, and entertainment. With all these advances in multimedia coding and communication technologies over the past decade, the major hurdle for allowing much broader access of multimedia assets and deployment of multimedia services no longer lies with bandwidth-related issues, but with assuring that content is used for its intended purpose by its intended recipients. The core issue now becomes the development of secure management of content usage and delivery across communication networks.

Data hiding and digital watermarking are promising new technologies for multimedia information protection and rights management. Secondary data can be embedded imperceptibly in digital multimedia signals for a variety of applications, including ownership protection, authentication, access control, and annotation. Data hiding can also be used to send side information in multimedia communication for achieving additional functionalities or enhancing performance. The extraction of the embedded data may or may not need knowledge of the original host media data. In addition to imperceptibility, robustness against moderate processing such as compression is also an important consideration. The requirements of imperceptibility, robustness and the hiding of maximum number of bits are basic for many data hiding applications. To satisfy these conflicting requirements, attention must be paid to the visual and hearing perception model and the types of media

data, viz. speech, music, line drawings, signature, natural image, etc. In addition, different parts of the media data may have significantly different embedding capacity. How to handle this uneven distribution of capacity is also a challenge. Another concern of data hiding is the protection against intentional attacks, attempts aimed at remove or obliterate the hidden data or watermark.

This book, based on the Ph.D. dissertation of the first author [46], addresses both theoretical and practical aspects of multimedia data hiding, and tackles both design and attack problems. It is organized into three parts: *Fundamental Issues*, *Algorithm and System Designs*, and *Attacks and Countermeasures*.

In the fundamental part, we identify the key elements of data hiding through a layered structure. Data hiding is modeled as a communication problem where the embedded data is the signal to be transmitted. The tradeoff of robustness versus capacity is studies for two major categories of embedding mechanisms. In addition, a comprehensive solution is proposed to address the problem caused by the unevenly distributed embedding capacity. The question of constant bit rate versus variable bit rate hiding is also addressed.

In the design part, we present new data hiding algorithms for binary images, grayscale and color images, and videos. A variety of applications are covered, including annotation, tamper detection, copy/access control, fingerprinting, and ownership protection. These designs provide concrete examples regarding the choice of embedding mechanisms, the selection of modulation/multiplexing technique(s) for hiding multiple bits, and the handling of uneven embedding capacity. The use of data hiding in video communication to convey side information for additional functionalities or better performance is demonstrated by the novel approaches for real-time transcoding and error concealment.

Many data hiding applications operate in a competitive environment where an adversary has an incentive to remove or obliterate the embedded data. Thus the testing of the robustness and security via attacks is important. In the last part of the book, we discuss a number of attacks and countermeasures for data hiding systems. The discussion begins with three specific types of watermarking schemes, in which full knowledge of the watermarking algorithms is available. Attention is then turned to the attack problems for digital music under a unique competitive environment, in which the watermarking algorithms are unknown to analysts. This work is based on our participation in the recent public challenge in the form of attacking four audio watermarking technologies of the Secure Digital Music Initiative (SDMI).

Min Wu and Bede Liu *Princeton, New Jersey*
June 2002

http://www.springer.com/978-0-387-95426-4

Multimedia Data Hiding
Wu, M.; Liu, B.
2003, XIX, 219 p. 55 illus., Hardcover
ISBN: 978-0-387-95426-4