EURASIP Book Series on Signal Processing and Communications

Multimedia Fingerprinting Forensics for Traitor Tracing

K. J. Ray Liu, Wade Trappe, Z. Jane Wang,
Min Wu, and Hong Zhao

Multimedia Fingerprinting Forensics for Traitor Tracing

EURASIP Book Series on Signal Processing and Communications, Volume 4

Multimedia Fingerprinting Forensics for Traitor Tracing

K. J. Ray Liu, Wade Trappe, Z. Jane Wang, Min Wu, and Hong Zhao

Hindawi Publishing Corporation
http://www.hindawi.com

EURASIP Book Series on Signal Processing and Communications
Editor-in-Chief: K. J. Ray Liu

Hindawi Publishing Corporation
410 Park Avenue, 15th Floor, #287 pmb, New York, NY 10022, USA
Nasr City Free Zone, Cairo 11816, Egypt
Fax: +1-866-HINDAWI (USA Toll-Free)

ISBN 977-5945-18-6

Dedication

To Our Families

Contents

Preface

Multimedia is becoming an integral part of our daily life. It is a means for us to communicate important information with each other, as well as a way to express our creative sides. The information and art contained inside media have economic value, personal value, and often broader impacts on the general welfare of our society. Consequently, multimedia is a form of digital information that must be protected.

This book is about protecting the economic and sensitive nature of multimedia. Since the Internet has become increasingly widespread, and now reaches into our everyday actions, it is easy to foresee that our modern communication networks will become the means for distributing multimedia content. This distribution will take many forms, ranging from a deceptively simple download-and-play model where a single consumer is the end-target for that content to streaming modes of operation where content is being enjoyed simultaneously by many consumers. Regardless of how you look at it, the future of multimedia is closely tied to the pervasiveness of our communication infrastructure. It therefore seems natural to protect multimedia by securing its distribution across these networks, that is, by employing the methods of network security.

Although securing the network and protecting the data crossing the network from eavesdropping is certainly essential for protecting multimedia, it is nonetheless a generic problem with generic solutions. Network security methods are important to many other applications, such as electronic commerce and computer security, in addition to being important to multimedia security. However, this book, *Multimedia Fingerprinting Forensics for Traitor Tracing*, is not about securing the communication infrastructure that will deliver multimedia.

Rather, this book focuses on the issue of protecting multimedia content when it is outside the realm of cryptography and network security. It is now relatively easy for adversaries to access multimedia content after it has been decrypted. Adversaries may now alter and repackage digital content. Therefore, ensuring that media content is employed by authorized users for its intended purpose, regardless of how it was delivered, is becoming an issue of eminent importance for both governmental security and commercial applications. As such, this book is about issues that are unique to multimedia and focuses specifically on how multimedia, unlike generic data types, can be protected by using fingerprint signals that are invisibly embedded inside the multimedia to trace and deter unauthorized content redistribution. That is, this book is about the rather nascent field of multimedia forensics, where the goal is to track and identify entities involved in the illegal manipulation and unauthorized usage of multimedia content. Ultimately, a solid foundation for media forensics will deter content fraud.

This book is targeted at an audience that is familiar with the fundamentals of multimedia signal processing and will teach the reader about the tools needed to build, analyze, and deploy solutions that will protect a variety of multimedia types. It, therefore, provides foundational material intended to assist the digital rights management (DRM) engineer understand technologies that complement traditional cryptographic security methods.

In this book, we will review a few major design methodologies for collusion-resistant fingerprinting of multimedia and highlight common and unique issues of various different fingerprinting techniques. The goal is to provide a broad overview of the recent advances in fingerprinting for tracing and identifying colluders. We will first provide background on robust data embedding, upon which multimedia fingerprinting system is built. We will then introduce the basic concepts of fingerprinting and collusion and provide a discussion on the various goals associated with fingerprint design and colluder tracing. Detailed discussions are then provided on two major classes of fingerprinting strategies, namely, orthogonal fingerprinting and correlated fingerprinting, where the latter involves the design of suitable codes that are employed with code modulation to create the fingerprints. As part of our discussion, we will arrive at a unified view of fingerprint design that covers orthogonal fingerprints, coded fingerprints, and other correlated fingerprints. After concluding the discussion of fingerprint design methodologies, we will explore two applications of fingerprinting. We will explore the migration of multimedia forensic technologies to networks, whereby the fingerprinting process will be integrated in core multicast functionality to provide DRM solution suitable for streaming delivery of content. Next, we will examine the protection of a type of multimedia content that has, until recently, been left unprotected by multimedia security solutions. In particular, we will explore the design of fingerprints for digital curves and maps and exploit the unique properties of digital curves in order to devise fingerprinting solutions.

We would like to thank Ms. Hongmei Gou, a Ph.D. student in the University of Maryland, for her contribution and involvement in preparing the draft of Chapter 8. The results presented in this book have been, in part, supported by the National Science Foundation and the Air Force Research Laboratories. We would like to thank these organizations for the support to explore and develop this exciting research area.

K. J. Ray Liu
Wade Trappe
Z. Jane Wang
Min Wu
Hong Zhao

1 Introduction

The ubiquity of high-bandwidth communication technologies, in combination with well-developed multimedia standards, has led to the proliferation of multimedia content in both the government and commercial sectors. We are witnessing the integration of next-generation multimedia standards, such as MPEG-4 [1, 2, 3, 4] and MPEG-7 [5], into software and hardware. As a result of this integration, users are able to readily create, manipulate, and combine multimedia content, such as audio clips and segments of video.

Multimedia data has become the mode by which we communicate with each other. We share digital photos with childhood friends whom we have not seen in years, and we share home videos of our children with our parents. Video conferences and the sharing of recorded presentations allow both corporate and governmental sectors to increase their productivity. It is now easier for artists to create their own cinema or record the performance of their garage-operated band. The combination of the availability of multimedia software and hardware with the availability of the Internet and the Web has encouraged artists, professional and amateur alike, to share their creative expressions. Ultimately, this has led to the creation of a digital marketplace.

Whether you examine the role of multimedia to convey information between different branches of the government, or you examine the role of multimedia in the digital marketplace, the picture is the same: the promise of multimedia is great, but its successful adoption stands on a dangerous precipice right now as the very technologies which facilitate its success also threaten its success. The combination of multimedia technologies and a pervasive communication infrastructure introduces an explosion of threats to the sharing of multimedia content. The tools that allowed users to create content, also allow them to duplicate or forge content. The medium that allowed users to share their expressions also facilitates the sharing of illicit or fraudulent content.

The alteration, repackaging, and redistribution of multimedia content pose a serious threat to both governmental security and commercial markets. The ability to securely and reliably exchange multimedia information is a strategic imperative in order for governments to operate smoothly. In order to facilitate the global

2 Preliminaries on data embedding

This chapter reviews the basics of robust data embedding. After a brief overview on digital watermarking and data embedding technologies, we steer our attention to a popular class of robust embedding techniques known as the spread-spectrum embedding. The detailed formulation on the embedding and detection aspects of the spread-spectrum technique establishes a foundation to unveil our technical discussions on multimedia fingerprinting in the subsequent chapters.

2.1. Content protection via digital watermarking

Multimedia content has both commercial and personal value that must be protected before one can share his/her work, or businesses can be founded to distribute and add value to their creations. Prior to digital multimedia content being put onto the network for delivery, the data can be modified to help protect the intellectual property of the content's creators and service providers. Encryption and data embedding are two complementary techniques for protecting multimedia content that have different goals. The primary goal behind encryption is confidentiality [29, 30, 31], that is, to provide access control so that only authorized users with the correct decryption keys can access the content. The protection provided by encryption terminates after decryption. Complementing this functionality, data embedding or digital watermarking associates a set of secondary data with the host media in a seamless way [17, 18]. The term "digital watermark" comes from an analogy to its analog counterpart: as an art of paper making, paper watermarks usually indicate the origin and the ownership, and/or establish the integrity and prevent counterfeiting. Similarly, digital watermarking has been considered in several real-world applications related to multimedia content protection and security. These include copy prevention for DVD and digital music, the assertion of ownership, the fingerprinting and tracing of content recipients, and the authentication of the content. While the protection provided by watermarks is usually passive, the embedded watermarks can travel with the host media and assume their protection function even after decryption. This capability of associating additional data with

3 Collusion attacks

Conventional embedding and watermarking techniques are typically concerned with robustness against a variety of attacks mounted by an individual. However, protecting the sanctity of digital fingerprints is no longer a traditional security issue with a single adversary. The global nature of the Internet has not only brought media closer to the consumers, but it has also brought adversaries closer to the media. It is now easy for a group of users with differently marked versions of the same content to come together and work together to mount attacks against the fingerprints. These attacks, known as collusion attacks, provide a cost-effective method for removing an identifying fingerprint and poses a significant threat to multimedia fingerprinting. For an improperly designed fingerprint, it is possible to gather a small coalition of colluders and sufficiently attenuate each of the colluders' identifying fingerprints to produce a new version of the content with no detectable traces. Thus, to design fingerprints that can resist collusion and identify the colluders, it is important to first model and analyze collusion and understand this new challenge in multimedia fingerprinting.

There are several types of collusion attacks that may be used against multimedia fingerprints. One method is simply to synchronize the media signals and average them, which is an example of the linear collusion attack. Another collusion attack, referred to as the copy-and-paste attack, involves users cutting out portions of each of their media signals and pasting them together to form a new signal. Other attacks may employ nonlinear operations, such as taking the maximum or median of the values of corresponding components of individual copies.

To uncover the underlying complexities governing the effect of nonlinear collusion attacks, this chapter conducts both analytical and experimental studies on the behavior of nonlinear collusion attacks. This study will serve as a guideline for later chapters where we jointly consider the issue of designing fingerprints, embedding fingerprints, and devising appropriate detection schemes that have the ability to robustly resist a broader spectrum of collusion attacks. We will build upon the discussion about using orthogonal modulation for fingerprinting that was provided in the previous chapter, and will focus our analysis of nonlinear collusion

4 Orthogonal fingerprinting and collusion resistance

We are interested in collusion-resistant fingerprinting technologies for protecting multimedia data. An early milestone work was presented in [77], addressing generic data fingerprinting using an underlying principle referred to as the *marking assumption*. However, multimedia data have very different characteristics from generic data and the marking assumption may not hold when fingerprinting multimedia data. In particular, fingerprints need to be embedded into media data. These differences have a critical impact on fingerprinting design.

There have been many technologies proposed in the literature to embed and hide fingerprints (watermarks) into different media. The combination of robustness [23, 24] and capacity [38, 39] has made additive spread-spectrum embedding a promising technique for protecting multimedia, and thus it was selected for our investigations. Though most watermarking methods are easy to defeat by collusion attacks, the spread-spectrum watermarking method proposed in [23], where the watermarks have a component-wise Gaussian distribution and are statistically independent, was argued to be highly resistant to collusion attacks [23, 70]. The basic intuition of this natural strategy is that the randomness inherent in such watermarks makes the probability of accusing an innocent user very unlikely. It was shown that randomness is needed to obtain collusion-resistance [78]. There are two main approaches to using spread spectrum for fingerprint embedding: orthogonal modulation originally proposed in [23], and code modulation. As reviewed earlier, *orthogonal modulation* [79] is a popular technique for watermarking and naturally lends itself to fingerprinting applications. The orthogonality or independence allows distinguishing the fingerprints to the maximum extent. The simplicity of encoding and embedding orthogonal fingerprints makes them attractive to applications involving a small group of users.

In order to facilitate the design of multimedia forensic systems for applications with different protection requirements, one critical research direction is evaluating the resistance performance of specific fingerprinting schemes when considering different types of attacks. Thus, it is essential to provide a fundamental understanding and analysis of collusion resistance for a specific fingerprinting system, where the main purpose is to study the relationships between the resistance

5 Group-oriented fingerprinting

In the previous chapter we have examined fingerprinting systems using orthogonal modulation. Despite the superior collusion resistance of orthogonal Gaussian fingerprints over other fingerprinting schemes, previous analysis revealed that attacks based on averaging a few dozen independent copies can confound a fingerprinting system using orthogonal modulation [58, 59, 69, 70]. Averaging collusion attack is proved effective on orthogonal fingerprinting system due to its effect on the energy reduction of the original fingerprints and the effect it has upon the detection performance. Therefore, by gathering a few dozen colluders, it is possible to sufficiently attenuate each colluder's identifying fingerprint and produce a new version of the content with no detectable fingerprints. Ultimately, for mass market consumption of multimedia, content will be distributed to thousands of users. In these scenarios, it is possible for a coalition of adversaries to acquire a few dozen copies of marked content, employ a simple average collusion attack, and thereby thwart the protection provided by the fingerprints. Thus, an alternative fingerprinting scheme is needed that will exploit a different aspect of the collusion problem in order to achieve improved collusion resistance.

We note that one major drawback of fingerprinting using orthogonal modulation is its severe energy reduction. For example, under the average attack, the resulting energy of the colluded copy is reduced to $1/K$ of the original fingerprint energy, with K being the number of colluders. This energy reduction significantly degrades the detection performance of each original fingerprint. As we mentioned earlier, there are two main approaches using spread spectrum for fingerprint embedding: orthogonal modulation and code modulation. The second option allows for constructing the fingerprint for each user as a linear combination of orthogonal noise-like basis signals. Along the code-modulation line, a key is to strategically introduce correlations into different fingerprints to allow accurate identification of the contributing fingerprints involved in collusion. The correlation concern also helps to decrease the energy reduction ratio observed in the case of orthogonal modulation. The resulting fingerprints can be based upon binary or real-valued code modulation. The group-oriented fingerprinting scheme studied

6 Anticollusion-coded (ACC) fingerprinting

In the previous chapters, we examined a conceptually simple strategy for fingerprinting that uses orthogonal signals as the fingerprints. We saw that the complexity of detection can be a concern for orthogonal fingerprints. Another problem with orthogonal fingerprinting arises when we examine the energy reduction in the fingerprint signals during collusion. Just looking at averaging collusion, it is easy to see that the energy reduction is roughly the same order of magnitude as the amount of colluders. This can be a significant problem for it means that once we have a few colluders, we become unlikely to identify any traitor. Further, another potential drawback with using orthogonal fingerprinting systems stems from the fact that the maximum number of users that can be supported by an orthogonal fingerprinting system is equal to the amount of orthogonal signals—that is, the dimensionality of the fingerprinting system can be a strict limit on the amount of copies of marked media that we distribute. In many commercial scenarios, the limitations imposed by using orthogonal fingerprinting is too restrictive, and it is therefore desirable to look for other fingerprinting strategies that can support a larger customer base, while also being able to resist collusion.

One natural approach to counteract the energy reduction caused by collusion is to introduce correlation between the fingerprints. When colluders combine their fingerprints, positively correlated components of the fingerprints will not experience as significant an energy reduction as would be experienced by orthogonal fingerprints. We have already seen an example of a fingerprinting strategy that uses correlated fingerprints. The group-based fingerprints that were introduced in Chapter 5 can be viewed as a special type of correlated fingerprints, where we employ a priori knowledge of the collusion pattern to guide us in introducing dependencies between fingerprints that assists in identifying collusion involving members of the same group. Further, by using an extra set of orthogonal signals to represent group information and introducing correlation, we were able to build more fingerprints than the amount of basis signals we had.

In this chapter, we will look at a more general approach for introducing dependency among the media fingerprints. We will build our fingerprints using code modulation, which is another modulation technique that is popular in digital

7 Secure fingerprint multicast for video streaming

The popular streaming technology enables the customers to enjoy multimedia on the fly and starts playing multimedia while parts of the data are still being transmitted. In video streaming applications, a huge amount of data has to be transmitted to a large number of users using limited bandwidth available under stringent latency constraints. To maximize their profit, video streaming service providers aim to reduce the communication cost in transmitting each copy, and therefore, to accommodate as many users as possible. Prior art in the literature usually utilizes the multicast technology that provides a bandwidth advantage for content and network providers when distributing the same data to multiple users [106, 152]. It reduces the overall communication cost by duplicating packages only when routing paths to multiple receivers diverge [106, 107].

For streaming applications that require traitor tracing capability, the uniqueness of each copy poses new challenges to the secure and efficient distribution of differently marked copies. Multicast cannot be directly applied to fingerprinting applications where different users receive slightly different copies. A simple solution of unicasting each fingerprinted copy is obviously inefficient since the bandwidth requirement grows linearly as the number of users increases while the difference between different copies is small. This calls for fingerprint multicast schemes that reduce the communication cost of distributing fingerprinted media without revealing the secrecy of the video content as well as that of the embedded fingerprints.

This chapter addresses the secure and efficient transmission of multimedia for video streaming with traitor tracing requirement. We first analyze the security requirement in video streaming and then investigate the fingerprint multicast techniques to efficiently distribute fingerprinted media to multiple users. To examine the performance of fingerprint multicast schemes, we use the pure unicast scheme as the benchmark in which each fingerprinted copy is unicasted to the corresponding user. For the fingerprint multicast schemes, we evaluate their bandwidth efficiency, the collusion resistance of the embedded fingerprints, and the perceptual quality of the reconstructed sequence at the decoder's side, and investigate the tradeoff between the communication cost and computation complexity.

8 Fingerprinting curves

This chapter presents a new data hiding method for curves. The proposed algorithm parameterizes a curve using the B-spline model and adds a spread-spectrum sequence to the coordinates of the B-spline control points. In order to achieve robust fingerprint detection, an iterative alignment-minimization algorithm is proposed to perform curve registration and to deal with the nonuniqueness of B-spline control points. We demonstrate through experiments the robustness of the proposed data hiding algorithm against various attacks such as collusion, cropping, geometric transformations, vector/raster-raster/vector conversions, printing and scanning, and some of their combinations. We also show the feasibility of our method for fingerprinting topographic maps as well as writings and drawings.

8.1. Introduction

Maps represent geospatial information ubiquitous in government, military, intelligence, and commercial operations. The traditional way of protecting a map from unauthorized copying and distribution is to place deliberate errors in the map, such as spelling "Nelson Road" as "Nelsen Road," bending a road in a wrong way, and/or placing a nonexisting pond. If an unauthorized user has a map containing basically the same set of errors, this is a strong piece of evidence on piracy that can be presented in court. One of the classic lawsuits is the Rockford Map Pub. versus Dir. Service Co. of Colorado, 768 F.2d 145, 147 (7th Cir., 1985), where phony middle initials of names in a map spelled out "Rockford Map Inc." when read from the top of the map to the bottom and thus copyright infringement was found. However, the traditional protection methods alter the geospatial meanings conveyed by a map, which can cause serious problems in critical government, military, intelligence, and commercial operations that require high-fidelity geospatial information. Furthermore, in the situations where distinct errors serve as fingerprints to trace individual copies, such deliberately placed errors can be easily identified and removed by computer programs after multiple copies of a map are brought to the digital domain. All these limitations of the traditional methods prompt for a modern way of map protection that can be more effective and less intrusive.

Bibliography

[1] J. L. Mitchell, W. B. Pennebaker, C. E. Fogg, and D. J. LeGall, *MPEG Video Compression Standard*, Chapman & Hall, New York, NY, USA, 1997.

[2] J. Chen, U. Koc, and K. J. R. Liu, *Design of Digital Video Coding Systems*, Marcel Dekker, New York, NY, USA, 2002.

[3] K. Ngan, C. Yap, and K. Tan, *Video Coding for Wireless Communication Systems*, Marcel Dekker, New York, NY, USA, 2001.

[4] A. Puri and T. Chen, Eds., *Multimedia Systems, Standards, and Networks*, Marcel Dekker, New York, NY, USA, 2000.

[5] MPEG committee, "MPEG-7 overview," ISO/IEC JTC1/SC29/WG11/N5525.

[6] S. Siwek, "Copyright industries in the U.S. economy, the 2002 report," Tech. Rep., International Intellectual Property Alliance (IIPA), Washington, DC, USA, 2002.

[7] The International Intellectual Property Alliance (IIPA).

[8] MPEG committee, "MPEG-21 overview," ISO/IEC JTC1/SC29/WG11/N4801.

[9] Secure Digital Music Initiative (SDMI), 2000.

[10] MPEG4 IPMP FPDAM, ISO/IEC 14 496-1: 2001/AMD3, ISO/IEC JTC 1/SC 29/WG11 N4701, March 2002.

[11] L. Tang, "Methods for encrypting and decrypting MPEG video data efficiently," in *Proc. 4th ACM International Conference on Multimedia (MULTIMEDIA '96)*, pp. 219–229, Boston, Mass, USA, November 1996.

[12] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 118–129, 2003.

[13] J. Wen, M. Severa, W. Zeng, M. H. Luttrell, and W. Jin, "A format-compliant configurable encryption framework for access control of video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 6, pp. 545–557, 2002.

[14] J. Song, R. Poovendran, W. Trappe, and K. J. R. Liu, "Dynamic key distribution scheme using data embedding for secure multimedia multicast," in *Security and Watermarking of Multimedia Contents III*, vol. 4314 of *Proceedings of SPIE*, pp. 618–628, Santa Clara, Calif, USA, January 2001.

[15] W. Trappe, J. Song, R. Poovendran, and K. J. R. Liu, "Key distribution for secure multimedia multicasts via data embedding," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '01)*, vol. 3, pp. 1449–1452, Salt Lake City, Utah, USA, May 2001.

[16] W. Trappe, J. Song, R. Poovendran, and K. J. R. Liu, "Key management and distribution for secure multimedia multicast," *IEEE Trans. Multimedia*, vol. 5, no. 4, pp. 544–557, 2003.

[17] I. J. Cox, J. A. Bloom, and M. L. Miller, *Digital Watermarking: Principles and Practice*, Morgan Kaufmann, San Francisco, Calif, USA, 2001.

[18] M. Wu and B. Liu, *Multimedia Data Hiding*, Springer, New York, NY, USA, 2003.

[19] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, no. 6, pp. 1064–1087, 1998.

[20] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[21] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, 1999.

[22] M. D. Swanson, B. Zhu, B. Chau, and A. H. Tewfik, "Object-based transparent video watermarking," in *Proc. IEEE 1st Workshop on Multimedia Signal Processing (MMSP '97)*, pp. 369–374, Princeton, NJ, USA, June 1997.

[23] I. J. Cox, J. Kilian, F. T. Leighton, and T. G. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[24] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Select. Areas Commun.*, vol. 16, no. 4, pp. 525–539, 1998.

[25] X. G. Xia, C. G. Boncelet, and G. R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, no. 12, pp. 497–511, 1998.

[26] W. Zhu, Z. Xiong, and Y.-Q. Zhang, "Multiresolution watermarking for images and video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 9, no. 4, pp. 545–550, 1999.

[27] D. Mukherjee, J. J. Chae, and S. K. Mitra, "A source and channel-coding framework for vector-based data hiding in video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 10, no. 4, pp. 630–645, 2000.

[28] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proc. IEEE*, vol. 87, no. 7, pp. 1108–1126, 1999.

[29] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1996.

[30] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Fla, USA, 1996.

[31] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, New York, NY, USA, 2001.

[32] J. A. Bloom, I. J. Cox, T. Kalker, J.-P. M. G. Linnartz, M. L. Miller, and C. B. S. Traw, "Copy protection for DVD video," *Proc. IEEE*, vol. 87, no. 7, pp. 1267–1276, 1999.

[33] J. Song, R. Poovendran, W. Trappe, and K. J. R. Liu, "Dynamic key distribution scheme using data embedding for secure multimedia multicast," in *Security and Watermarking of Multimedia Contents III*, vol. 4314 of *Proceedings of SPIE*, pp. 618–628, San Jose, Calif, USA, January 2001.

[34] P. Yin, B. Liu, and H. H. Yu, "Error concealment using data hiding," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '01)*, vol. 3, pp. 1453–1456, Salt Lake City, Utah, USA, May 2001.

[35] P. Yin, M. Wu, and B. Liu, "Robust error-resilient approach for MPEG video transmission over internet," in *Visual Communications and Image Processing*, vol. 4671 of *Proceedings of SPIE*, pp. 103–111, San Jose, Calif, USA, January 2002.

[36] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images," *IEEE Trans. Image Processing*, vol. 8, no. 11, pp. 1534–1548, 1999.

[37] M. Wu, H. Yu, and A. Gelman, "Multi-level data hiding for digital image and video," in *Multimedia Systems and Applications II*, vol. 3845 of *Proceedings of SPIE*, pp. 10–21, Boston, Mass, USA, September 1999.

[38] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 563–593, 2003.

[39] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[40] M. H. M Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. 29, no. 3, pp. 439–441, 1983.

[41] M. Kesal, M. K. Mihcak, R. Koetter, and P. Moulin, "Iteratively decodable codes for watermarking applications," in *Proc. 2nd International Symposium on Turbo Codes and Related Topics (ISTC '00)*, Brest, France, September 2000.

[42] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar Costa scheme for information embedding," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.

[43] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. Image Processing*, vol. 10, no. 5, pp. 767–782, 2001.

[44] J. Lubin, J. A. Bloom, and H. Cheng, "Robust content-dependent high-fidelity watermark for tracking in digital cinema," in *Security and Watermarking of Multimedia Contents V*, vol. 5020 of *Proceedings of SPIE*, pp. 536–545, Santa Clara, Calif, USA, June 2003.

[45] J. G. Proakis, *Digital Communications*, McGraw-Hill, New York, NY, USA, 4th edition, 2000.

[46] G. Csurka, F. Deguillaume, J. J. K. ÓRuanaidh, and T. Pun, "A Bayesian approach to affine transformation resistant image and video watermarking," in *Proc. 3rd Information Hiding Workshop (IHW '99)*, Lecture Notes in Computer Science, pp. 315–330, Hotel Elbflorenz, Dresden, Germany, September–October 1999.

[47] S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarks," in *Proc. 3rd Information Hiding Workshop (IHW '99)*, vol. 1768 of *Lecture Notes in Computer Science*, pp. 207–218, Hotel Elbflorenz, Dresden, Germany, September–October 1999.

[48] N. F. Johnson, Z. Duric, and S. Jajodia, "Recovery of watermarks from distorted images," in *Proc. 3rd Information Hiding Workshop (IHW '99)*, pp. 361–375, Hotel Elbflorenz, Dresden, Germany, September–October 1999.

[49] M. Alghoniemy and A. H. Tewfik, "Geometric distortion correction through image normalization," in *Proc. IEEE International Conference on Multimedia and Expo (ICME '00)*, vol. 3, pp. 1291–1294, New York, NY, USA, July–August 2000.

[50] M. Wu, W. Trappe, Z. J. Wang, and K. J. R. Liu, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Processing Mag.*, vol. 21, no. 2, pp. 15–27, 2004.

[51] K. Su, D. Kundur, and D. Hatzinakos, "A content dependent spatially localized video watermark for resistance to collusion and interpolation attacks," in *Proc. IEEE International Conference on Image Processing (ICIP '01)*, vol. 1, pp. 818–821, Thessaloniki, Greece, October 2001.

[52] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE J. Select. Areas Commun.*, vol. 16, no. 4, pp. 540–550, 1998.

[53] D. Kirovski and F. A. P. Petitcolas, "Blind pattern matching attack on watermarking systems," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 1045–1053, 2003.

[54] H. V. Poor, *An Introduction to Signal Detection and Estimation*, Springer, New York, NY, USA, 2nd edition, 1999.

[55] M. Wu, H. Yu, and B. Liu, "Data hiding in image and video. II. Designs and applications," *IEEE Trans. Image Processing*, vol. 12, no. 6, pp. 696–705, 2003.

[56] S. V. Voloshynovskiy, F. Deguillaume, S. Pereira, and T. Pun, "Optimal adaptive diversity watermarking with channel state estimation," in *Security and Watermarking of Multimedia Contents III*, vol. 4314 of *Proceedings of SPIE*, pp. 673–685, San Jose, Calif, USA, January 2001.

[57] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Trans. Image Processing*, vol. 9, no. 1, pp. 55–68, 2000, *Special Issue on Image and Video Processing for Digital Libraries*.

[58] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *IEEE Trans. Image Processing*, vol. 14, no. 6, pp. 804–821, 2005.

[59] Z. J. Wang, M. Wu, H. Zhao, K. J. R. Liu, and W. Trappe, "Resistance of orthogonal Gaussian fingerprints to collusion attacks," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '03)*, vol. 4, pp. 724–727, Hong Kong, China, April 2003.

[60] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Nonlinear collusion attacks on independent fingerprints for multimedia," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '03)*, vol. 5, pp. 664–667, Hong Kong, China, April 2003.

[61] H. D. Brunk, *An Introduction to Mathematical Statistics*, Ginn and Company, Boston, Mass, USA, 1960.

[62] H. Stone, "Analysis of attacks on image watermarks with randomized coefficients," Tech. Rep. 96-045, NEC Research Institute, Princeton, NJ, USA, 1996.

[63] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," in *Proc. International Conference on Image Processing (ICIP '96)*, vol. 3, pp. 211–214, Lausanne, Switzerland, September 1996.

[64] H. A. Peterson, A. J. Ahumada Jr., and A. B. Watson, "An improved detection model for DCT coefficient quantization," in *Human Vision, Visual Processing, and Digital Display IV*, vol. 1913 of *Proceedings of SPIE*, pp. 191–201, Bellingham, Wash, USA, February 1993.

[65] A. B. Watson, "DCT quantization matrices visually optimized for individual images," in *Human Vision, Visual Processing, and Digital Display IV*, vol. 1913 of *Proceedings of SPIE*, pp. 202–216, San Jose, Calif, USA, February 1993.

[66] Joint Photographic Experts Group (JPEG).

[67] G. K. Wallace, "The JPEG still picture compression standard," *IEEE Trans. Consumer Electron.*, vol. 38, no. 1, pp. 18–34, 1992.

[68] B. Tao and B. Dickinson, "Adaptive watermarking in the DCT domain," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '97)*, vol. 4, pp. 2985–2988, Munich, Germany, April 1997.

[69] F. Ergun, J. Kilian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," in *Advances in Cryptology (Eurocrypt '99)*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 140–149, Prague, Czech Republic, May 1999.

[70] J. Kilian, F. T. Leighton, L. R. Matheson, T. G. Shamoon, R. Tajan, and F. Zane, "Resistance of digital watermarks to collusive attacks," Tech. Rep. TR-585-98, Department of Computer Science, Princeton University, Princeton, NJ, USA, 1998.

[71] S. He and M. Wu, "Improving collusion resistance of error correcting code based multimedia fingerprinting," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '05)*, vol. 2, pp. 1029–1032, Philadelphia, Pa, USA, March 2005.

[72] J. Su, J. Eggers, and B. Girod, "Capacity of digital watermarks subjected to an optimal collusion attack," in *Proc. 10th European Signal Processing Conference (EUSIPCO '00)*, Tampere, Finland, September 2000.

[73] S. Craver, B. Liu, and W. Wolf, "Histo-cepstral analysis for reverse-engineering watermarks," in *Proc. 38th Conference on Information Sciences and Systems (CISS '04)*, pp. 824–826, Princeton, NJ, USA, March 2004.

[74] H. A. David, *Order Statistics*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1981.

[75] W. Gander and W. Gautschi, "Adaptive quadrature—revisited," *BIT Numerical Mathematics*, vol. 40, no. 1, pp. 84–101, 2000.

[76] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Performance of detection statistics under collusion attacks on independent multimedia fingerprints," in *Proc. IEEE International Conference on Multimedia and Expo (ICME '03)*, vol. 1, pp. 205–208, Baltimore, Md, USA, July 2003.

[77] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.

[78] F. Zane, "Efficient watermark detection and collusion security," in *Proc. Financial Cryptography (FC '00)*, vol. 1962 of *Lecture Notes in Computer Science*, pp. 21–32, Anguilla, British West Indies, February 2000.

[79] M. Wu and B. Liu, "Data hiding in image and video. I. Fundamental issues and solutions," *IEEE Trans. Image Processing*, vol. 12, no. 6, pp. 685–695, 2003.

[80] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Processing*, vol. 51, no. 4, pp. 1069–1087, 2003, Special Issue on Signal Processing for Data Hiding in Digital Media.

[81] M. K. Simon, S. M. Hinedi, and W. C. Lindsey, "Appendix 3b: the Gaussian integral $q(x)$," in *Digital Communication Techniques: Signal Design and Detection*, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.

[82] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Trans. Image Processing*, vol. 14, no. 5, pp. 646–661, 2005.

[83] A. Herrigel, J. J. K. ÓRuanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure copyright protection techniques for digital images," in *Proc. 2nd Information Hiding Workshop (IHW '98)*, vol. 1525 of *Lecture Notes in Computer Science*, pp. 169–190, Portland, Ore, USA, April 1998.

[84] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*, McGraw-Hill, New York, NY, USA, 1989.

[85] J. A. Aslam and A. Dhagat, "Searching in the presence of linearly bounded errors," in *Proc. 23rd Annual ACM Symposium on Theory of Computing (STOC '91)*, pp. 486–493, ACM Press, New Orleans, La, USA, May 1991.

[86] D.-Z. Du, G.-L. Xue, S.-Z. Sun, and S.-W. Cheng, "Modifications of competitive group testing," *SIAM Journal on Computing*, vol. 23, no. 1, pp. 82–96, 1994.

[87] D.-Z. Du and H. Park, "On competitive group testing," *SIAM Journal on Computing*, vol. 23, no. 5, pp. 1019–1025, 1994.

[88] M. Wu and B. Liu, "Modulation and multiplexing techniques for multimedia data hiding," in *Multimedia Systems and Applications IV*, vol. 4518 of *Proceedings of SPIE*, pp. 228–238, Denver, Colo, USA, August 2001.

[89] E. Lehmann, *Adaptive Filter Theory*, Prentice Hall, Englewood Cliffs, NJ, USA, 1996.

[90] N. Balakrishnan and C. Rao, *Order Statistics: Theory and Methods*, Elsevier Science, Amsterdam, the Netherlands, 1998.

[91] H. Stark and J. Woods, *Probability and Random Processes with Applications to Signal Processing*, Prentice Hall, New York, NY, USA, 3rd edition, 2002.

[92] Y. Yacobi, "Improved Boneh-Shaw content fingerprinting," in *Topics in Cryptology—CT-RSA 2001, The Cryptographer's Track at RSA Conference (CT-RSA '01)*, vol. 2020 of *Lecture Notes in Computer Science*, pp. 378–391, San Francisco, Calif, USA, April 2001.

[93] W. Trappe, M. Wu, and K. J. R. Liu, "Collusion-resistant fingerprinting for multimedia," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '02)*, vol. 4, pp. 3309–3312, Orlando, Fla, USA, May 2002.

[94] J. H. Dinitz and D. R. Stinson, *Contemporary Design Theory: A Collection of Surveys*, John Wiley & Sons, New York, NY, USA, 1992.

[95] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, Fla, USA, 1996.

[96] J. Dittmann, P. Schmitt, E. Saar, J. Schwenk, and J. Ueberberg, "Combining digital watermarks and collusion secure fingerprints for digital images," *SPIE Journal of Electronic Imaging*, vol. 9, no. 4, pp. 456–467, 2000.

[97] C. C. Lindner and C. A. Rodger, *Design Theory*, CRC Press, Boca Raton, Fla, USA, 1997.

[98] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, UK, 1994.

[99] S. F. Yau and Y. Bresler, "Maximum likelihood parameter estimation of superimposed signals by dynamic programming," *IEEE Trans. Signal Processing*, vol. 41, no. 2, pp. 804–820, 1993.

[100] I. Ziskind and M. Wax, "Maximum likelihood localization of multiple sources by alternating projection," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. 36, no. 10, pp. 1553–1560, 1988.

[101] T. G. Manickam, R. J. Vaccaro, and D. W. Tufts, "A least-squares algorithm for multipath time-delay estimation," *IEEE Trans. Signal Processing*, vol. 42, no. 11, pp. 3229–3233, 1994.

[102] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Anti-collusion of group-oriented fingerprinting," in *Proc. IEEE International Conference on Multimedia and Expo (ICME '03)*, vol. 2, pp. 217–220, Baltimore, Md, USA, July 2003.

[103] Z. Li and W. Trappe, "Collusion-resistant fingerprints from WBE sequence sets," to appear in *Proc. IEEE International Conference on Communications (ICC '05)*, Seoul, Korea, May 2005.

[104] M. Ajtai, "The shortest vector problem in L_2 is NP-Hard for randomized reductions," in *Proc. 30th Annual ACM Symposium on Theory of Computing (STOC '98)*, pp. 10–19, Dallas, Tex, USA, May 1998.

[105] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of Computation*, vol. 44, no. 4, pp. 463–471, 1985.

[106] S. Paul, *Multicast on the Internet and Its Application*, Kluwer Academic, Boston, Mass, USA, 1998.

[107] R. C. Chalmers and K. C. Almeroth, "Modeling the branching characteristics and efficiency gains in global multicast trees," in *Proc. 20th IEEE Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '01)*, vol. 1, pp. 449–458, Anchorage, Alaska, USA, April 2001.

[108] H. Zhao and K. J. R. Liu, "Fingerprint multicast in secure video streaming," to appear in *IEEE Trans. Image Processing*, Fall 2005.

[109] C. Pfleeger, *Security in Computing*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 1996.

[110] I. J. Cox and J.-P. M. G. Linnartz, "Some general methods for tampering with watermarks," *IEEE J. Select. Areas Commun.*, vol. 16, no. 4, pp. 587–593, 1998.

[111] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," in *Security and Watermarking of Multimedia Contents, Electronic Imaging*, vol. 3657 of *Proceedings of SPIE*, pp. 147–158, San Jose, Calif, USA, April 1999.

[112] H.-H. Chu, L. Qiao, and K. Nahrstedt, "A secure multicast protocol with copyright protection," *ACM SIGCOMM Computer Communications Review*, vol. 32, no. 2, pp. 42–60, 2002.

[113] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proc. IEEE*, vol. 92, no. 6, pp. 918–932, 2004.

[114] I. Brown, C. Perkins, and J. Crowcroft, "Watercasting: Distributed watermarking of multicast media," in *Proc. 1st International Workshop on Networked Group Communication (NGC '99)*, pp. 286–300, Pisa, Italy, November 1999.

[115] G. Caronni and C. Schuba, "Enabling hierarchical and bulk-distribution for watermarked content," in *Proc. 17th Annual Computer Security Applications Conference (ACSAC '01)*, pp. 277–285, New Orleans, La, USA, December 2001.

[116] D. Konstantas and D. Thanos, "Commercial dissemination of video over open networks: issues and approaches," Tech. Rep., Object Systems Group, Center Universitaire d'Informatique of University of Geneva, Geneva, Switzerland, 2000.

[117] R. Parviainen and R. Parnes, "Enabling hierarchical and bulk-distribution for watermarked content," in *Proc. IFIP TC6/TC11 International Conference on Communications and Multimedia Security Issues*, vol. 192, Darmstadt, Germany, May 2001.

[118] P. Judge and M. Ammar, "WHIM: Watermarking multicast video with a hierarchy of intermediaries," in *Proc. 10th International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV '00)*, Chapel Hill, NC, USA, June 2000.

[119] T. Wu and S. F. Wu, "Selective encryption and watermarking of MPEG video," in *Proc. International Conference on Imaging Science, Systems, and Technology (CISST '97)*, Las Vegas, Nev, USA, June–July 1997.

[120] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP Journal on Applied Signal Processing*, vol. 2004, no. 14, pp. 2153–2173, 2004.

[121] H. Zhao and K. J. R. Liu, "Bandwidth efficient fingerprint multicast for video streaming," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '04)*, vol. 5, pp. 849–852, Montreal, Quebec, Canada, May 2004.

[122] M. Wu and Y. Mao, "Communication-friendly encryption of multimedia," in *IEEE Workshop on Multimedia Signal Processing (MMSP '02)*, pp. 292–295, St. Thomas, Virgin Islands, USA, December 2002.

[123] L. Qiao and K. Nahrstedt, "A new algorithm for MPEG video encryption," in *Proc. International Conference on Imaging Science, Systems and Technology (CISST '97)*, pp. 21–29, Las Vegas, Nev, USA, June 1997.

[124] H. Zhao and K. J. R. Liu, "A secure multicast scheme for anti-collusion fingerprinted video," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM '04)*, vol. 2, pp. 571–575, Dallas, Tex, USA, November–December 2004.

[125] J. C.-I. Chuang and M. A. Sirbu, "Pricing multicast communication: A cost-based approach," *Telecommunication Systems*, vol. 17, no. 3, pp. 281–297, 2001.

[126] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing*, vol. 66, no. 3, pp. 283–301, 1998.

[127] H.-H. Chang, T. Chen, and K.-S. Kan, "Watermarking 2D/3D graphics for copyright protection," in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '03)*, vol. 4, pp. 720–723, Hong Kong, China, April 2003.

[128] M. Barni, F. Bartolini, A. Piva, and F. Salucco, "Robust watermarking of cartographic images," *EURASIP Journal on Applied Signal Processing*, vol. 2002, no. 2, pp. 197–208, 2002.

[129] V. Solachidis and I. Pitas, "Watermarking polygonal lines using Fourier descriptors," *IEEE Comput. Graph. Appl.*, vol. 24, no. 3, pp. 44–51, 2004.

[130] R. Ohbuchi, H. Ueda, and S. Endoh, "Watermarking 2D vector maps in the mesh-spectral domain," in *Proc. Shape Modeling International (SMI '03)*, pp. 216–228, Seoul, Korea, May 2003.

[131] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," in *Proc. International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, pp. 242–251, Vienna, Austria, August 1995.

[132] M. Wu, E. Tang, and B. Lin, "Data hiding in digital binary image," in *Proc. IEEE International Conference on Multimedia and Expo (ICME '00)*, vol. 1, pp. 393–396, New York, NY, USA, July–August 2000.

[133] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, 2004.

[134] K. Matsui and K. Tanaka, "Video-steganography: how to secretly embed a signature in a picture," *IMA Intellectual Property Project Proceedings*, vol. 1, no. 1, pp. 187–205, 1994.

[135] N. F. Maxemchuk and S. Low, "Marking text documents," in *Proc. IEEE International Conference on Image Processing (ICIP '97)*, vol. 3, pp. 13–13, Santa Barbara, Calif, USA, October 1997.

[136] R. Ohbuchi, H. Masuda, and M. Aono, "A shape-preserving data embedding algorithm for NURBS curves and surfaces," in *Proc. Computer Graphics International (CGI '99)*, pp. 180–188, Canmore, Canada, June 1999.

[137] J. J. Lee, N. I. Cho, and J. W. Kim, "Watermarking for 3D NURBS graphic data," in *Proc. IEEE Workshop on Multimedia Signal Processing (MMSP '02)*, pp. 304–307, St. Thomas, Virgin Islands, USA, December 2002.

[138] J. J. Lee, N. I. Cho, and S. U. Lee, "Watermarking algorithms for 3D nurbs graphic data," *EURASIP Journal on Applied Signal Processing*, vol. 2004, no. 14, pp. 2142–2152, 2004.

[139] K. H. Ko, T. Maekawa, N. M. Patrikalakis, H. Masuda, and F.-E. Wolter, "Shape intrinsic fingerprints for free-form object matching," in *Proc. 8th ACM Symposium on Solid Modeling and Applications*, pp. 196–207, Seattle, Wash, USA, June 2003.

[140] H. Gou and M. Wu, "Data hiding in curves with applications to map fingerprinting," *to appear in IEEE Trans. on Image Processing*, Special Issue on Secure Media, October 2005.

[141] H. Gou and M. Wu, "Data hiding in curves for collusion-resistant digital fingerprinting," in *Proc. IEEE International Conference on Image Processing (ICIP '04)*, vol. 1, pp. 51–54, Singapore, October 2004.

[142] H. Gou and M. Wu, "Fingerprinting curves," in *Proc. IEEE International Workshop on Digital Watermarking (IWDW '04)*, pp. 13–28, Seoul, Korea, October–November 2004.

[143] A. K. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall, Englewood Cliffs, NJ, USA, 1989.

[144] G. E. Farin, *Curves and Surfaces for Computer-Aided Geometric Design: A Practical Guide*, Academic Press, New York, NY, USA, 4th edition, 1997.

[145] D. Kirovski, H. S. Malvar, and Y. Yacobi, "Multimedia content screening using a dual watermarking and fingerprinting system," in *Proc. ACM Multimedia*, pp. 372–381, Juan Les Pins, France, December 2002.

[146] Z. Huang and F. S. Cohen, "Affine-invariant B-spline moments for curve matching," *IEEE Trans. Image Processing*, vol. 5, no. 10, pp. 1473–1480, 1996.

[147] C. A. Cabrelli and U. M. Molter, "Automatic representation of binary images," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 12, no. 12, pp. 1190–1196, 1990.

[148] H. S. M. Coxeter, *Introduction to Geometry*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1969.

[149] F. S. Cohen and J.-Y. Wang, "Part I: Modeling image curves using invariant 3-D object curve models-a path to 3-D recognition and shape estimation from image contours," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 16, no. 1, pp. 1–12, 1994.

[150] E. Belogay, C. A. Cabrelli, U. M. Molter, and R. Shonkwiler, "Calculating the Hausdorff distance between curves," *Information Processing Letters*, vol. 64, no. 1, pp. 17–22, 1997.

[151] M. Xia and B. Liu, "Image registration by "Super-curves"," *IEEE Trans. Image Processing*, vol. 13, no. 5, pp. 720–732, 2004.

[152] U. Varshney, "Multicast over wireless networks," *Communications of the ACM*, vol. 45, no. 12, pp. 31–37, 2002.

Index