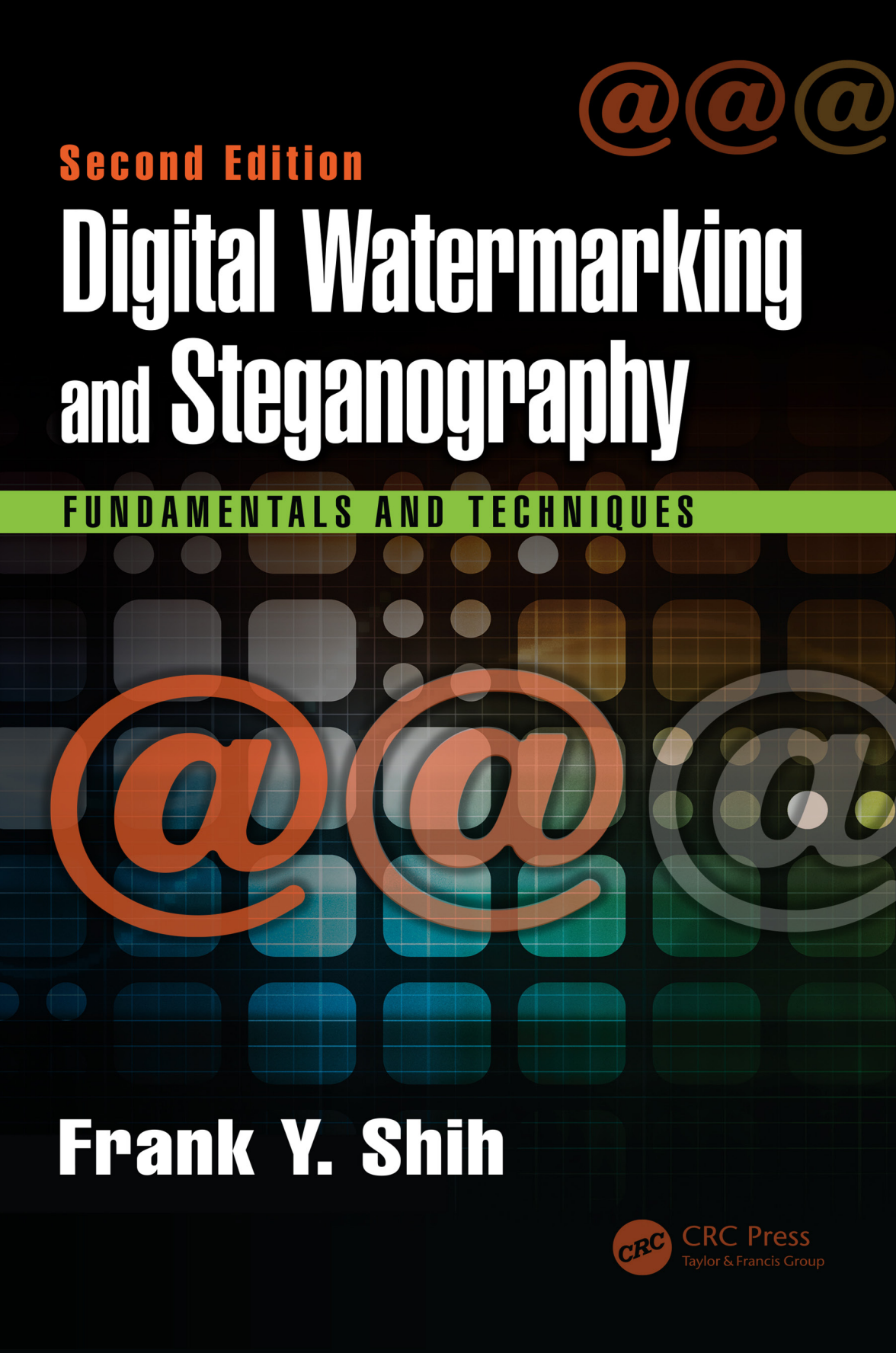
Second Edition
Digital Watermarking and Steganography
FUNDAMENTALS AND TECHNIQUES
Frank Y. Shih
CRC Press
Taylor & Francis Group

Digital Watermarking and Steganography: Fundamentals and Techniques (Second Edition)

Digital Watermarking and Steganography: Fundamentals and Techniques (Second Edition)

Frank Y. Shih
New Jersey Institute of Technology

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper

International Standard Book Number-13: 978-1-4987-3876-7 (Hardback)

Library of Congress Cataloging-in-Publication Data

Names: Shih, Frank Y., author.
Title: Digital watermarking and steganography : fundamentals and techniques / Frank Y. Shih.
Description: Second edition. | Boca Raton : Taylor & Francis, CRC Press, 2017. | Includes bibliographical references.
Identifiers: LCCN 2016048478| ISBN 9781498738767 (hardback : alk. paper) | ISBN 9781498738774 (ebook)
Subjects: LCSH: Digital watermarking. | Data encryption (Computer science) | Computer security. | Multimedia systems--Security measures. | Intellectual property.
Classification: LCC QA76.9.A25 S467 2017 | DDC 005.8/2--dc23
LC record available at https://lccn.loc.gov/2016048478

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Dedication

To my loving wife and children, to my parents who encouraged me through the years, and to those who helped me in the process of writing this book.

Contents

Preface

Digital watermarking and steganography are important topics because digital multimedia is widely used and the Internet is rapidly growing. This book intends to provide a comprehensive overview of the different aspects, mechanisms, and techniques of information security. It is written for students, researchers, and professionals who take the related courses, want to improve their knowledge, and want to gain experience in digital watermarking and steganography.

Digital watermarking technology can be used to guarantee authenticity and as proof that the content has not been altered since insertion. Steganographic messages are often first encrypted by some traditional means, and then a covert text is modified in some way to contain the encrypted message. The need for information security exists everywhere, everyday.

This book aims to provide students, researchers, and professionals with technical information regarding digital watermarking and steganography, as well as instruct them on the fundamental theoretical framework for developing the extensive advanced techniques. By comprehensively considering the essential principles of the digital watermarking and steganographic systems, one can not only obtain novel ideas about implementing advanced algorithms but also discover new problems. The principles of digital watermarking and steganography in this book are illustrated with plentiful graphs and examples in order to simplify the problems, so readers can easily understand even complicated theories.

Several robust algorithms are presented in this book to illustrate the framework and to provide assistance and tools for understanding and implementing the fundamental principles. The combined spatial and frequency domain watermarking technique provides a new method of enlarging the embedding capacity of watermarks. The genetic algorithm (GA)-based watermarking technique solves the rounding error problem and is an efficient approach to embedding. The adjusted-purpose watermarking technique simplifies the selection of different types, and can be integrated into other watermarking techniques. The robust high-capacity watermarking technique successfully enlarges the hiding capacity while maintaining the watermark's robustness. GA-based steganography provides a new way of developing a robust steganographic system by artificially counterfeiting statistical features instead of using the traditional strategy of avoiding the alteration of statistical features.

OVERVIEW OF THE BOOK

In Chapter 1, digital watermarking and digital steganography are briefly introduced. Then, the difference between watermarking and steganography is addressed. Next, a brief history along with updates on recently published resources is provided. The rest of the book is broken into two parts: Chapters 2 through 10 cover digital watermarking, and Chapters 11 and 12 cover digital steganography.

In Chapter 2, digital watermarking techniques are categorized, based on their characteristics, into five pairs: blind versus nonblind, perceptible versus imperceptible,

private versus public, robust versus fragile, and spatial domain versus frequency domain. Digital watermarking techniques are classified, based on their applications, into five types: copyright protection, data authentication, fingerprinting, copy control, and device control. In Chapter 3, the basic mathematical preliminaries are introduced, including least-significant-bit substitution, the discrete Fourier transform, the discrete cosine transform, the discrete wavelet transform, random sequence generation, chaotic maps, error correction code, and set partitioning in hierarchical trees. In Chapter 4, the fundamentals of digital watermarking are introduced. The subject is divided into four classes: spatial domain, frequency domain, fragile, and robust. In the spatial domain class, substitutive watermarking and additive watermarking are introduced. In the frequency domain class, substitutive watermarking, multiplicative watermarking, vector quantization watermarking, and the rounding error problem are introduced. In the fragile watermark class, block-based watermarks, their weaknesses, and hierarchy-based watermarks are described. In the robust watermark class, the redundant embedding approach and spread spectrum are discussed.

In Chapter 5, the issue of watermarking attacks is explored. The attacks are summarized into four types: image-processing attacks, geometric attacks, cryptographic attacks, and protocol attacks. Then, they are further divided into four classes: filtering, remodulation, JPEG coding distortion, and JPEG 2000 compression. Next, geometric attacks are divided into nine classes: image scaling, rotation, image clipping, linear transformation, bending, warping, perspective projection, collage, and templates. After that, the cryptographic and protocol attacks are explained, and the available watermarking tools are provided. In the end, an efficient block-based fragile watermarking system is presented for tamper localization and the recovery of images. In Chapter 6, the technique of combinational digital watermarking is introduced. The combination of the spatial and frequency domains is described, and its advantages and experimental results are provided. The further encryption of combinational watermarks is explained. Chapter 7 shows how GAs can be applied to digital watermarking. The concept and basic operations of GAs are introduced and fitness functions are discussed. Then, GA-based rounding error correction watermarking is introduced. Next, the application of GA-based algorithms to medical image watermarking is presented. At the end of the chapter, the authentication of JPEG images based on GAs is described.

In Chapter 8, the technique of adjusted-purpose digital watermarking is introduced. Following an overview, the morphological approach to extracting pixel-based features, strategies for adjusting the variable-sized transform window (VSTW), and the quantity factor (QF) are presented. How VSTW is used to determine whether the embedded strategy should be in the spatial or the frequency domain and how the QF is used to choose fragile, semifragile, or robust watermarks are explained. An optimal watermarking solution is presented that considers imperceptibility, capacity, and robustness by using particle swarm optimization. Chapter 9 introduces a technique for robust high-capacity digital watermarking. After the weaknesses of current robust watermarking are pointed out, the concept of robust watermarking is introduced. Following this, the processes of enlarging the significant coefficients and breaking the local spatial similarity are explained. Next, new concepts are presented concerning block-based chaotic maps and the determination of embedding locations.

The design of intersection-based pixel collection, reference registers, and containers is described. A robust high-capacity watermarking algorithm and its embedding and extracting procedures are introduced. Experimental results are provided to explore capacity enlargement, robust experiments, and performance comparisons. At the end of the chapter, the technique of high-capacity multiple-regions-of-interest watermarking for medical images is presented. Chapter 10 introduces a novel fragile watermark-based reversible image authentication scheme. The chaotic hash value of each image block is computed as the watermark, which ensures that there is complicated nonlinear and sensitive dependence within the image's gray features, the secret key, and the watermark. Reversible watermark embedding allows the original image to be recovered exactly after the authentication message has been extracted. An improved reversible data-hiding algorithm using multiple scanning techniques and histogram modification is presented.

Chapters 11 and 12 cover the topic of digital steganography. In Chapter 11, three types of steganography are introduced: technical, linguistic, and digital. Some applications of steganography are illustrated, including convert communication and one-time pad communication. Concerns about embedding security and imperceptibility are explained. Four examples of steganography software are given: S-Tools, StegoDos, EzStego, and JSteg-Jpeg. Next, the concept of steganalysis, which intends to attack steganography, is discussed. The statistical properties of images, the visual steganalytic system (VSS), and the IQM-based steganalytic system are described. Three learning strategies—support vector machines, neural networks, and principle component analysis—are reviewed. At the end of the chapter, the frequency domain steganalytic system (FDSS) is presented. In Chapter 12, steganography based on GAs and differential evolution (DE) is introduced, which can break steganalytic systems. The emphasis is shifted from traditionally avoiding the alteration of statistical features to artificially counterfeiting them. An overview of GA-based breaking methodology is first presented. Then, GA-based breaking algorithms in the spatial domain steganalytic system (SDSS) are described. How one can generate stego-images in the VSS and in the IQM-based steganalytic system are explained. Next, the strategy of GA-based breaking algorithms in the FDSS is provided. Experimental results show that this algorithm can not only pass the detection of steganalytic systems but also increase the capacity of the embedded message and enhance the peak signal-to-noise ratio of stego-images. At the end of the chapter, we present the techniques of DE-based steganography. DE is a relative latecomer, but its popularity has been catching up. It is fast in numerical optimization and is more likely to find the true optimum.

FEATURES OF THE BOOK

- New state-of-the-art techniques for digital watermarking and steganography
- Numerous practical examples
- A more intuitive development and a clear tutorial on the complex technology
- An updated bibliography
- Extensive discussion on watermarking and steganography
- The inclusion of steganalytic techniques and their counterexamples

FEEDBACK ON THE BOOK

It is my hope that there will be opportunities to correct any errors in this book; therefore, please provide a clear description of any errors that you may find. Your suggestions on how to improve the book are always welcome. For this, please use either e-mail (shih@njit.edu) or regular mail to the author: Frank Y. Shih, College of Computing Sciences, New Jersey Institute of Technology, University Heights, Newark, NJ 07102-1982.

Acknowledgments

Portions of the book appeared in earlier forms as conference papers, journal papers, or theses with my students here at the New Jersey Institute of Technology. Therefore, these parts of the text are sometimes a combination of my words and those of my students. I would like to gratefully acknowledge the Institute of Electrical and Electronic Engineers (IEEE) and Elsevier for giving me permission to reuse texts and figures that have appeared in some of my past publications.

Frank Y. Shih
New Jersey Institute of Technology

Author

Frank Y. Shih received a BS from National Cheng-Kung University, Taiwan, in 1980, an MS from the State University of New York at Stony Brook in 1984, and a PhD from Purdue University, West Lafayette, Indiana, in 1987, all in electrical and computer engineering. He is jointly appointed as a professor in the Department of Computer Science, the Department of Electrical and Computer Engineering, and the Department of Biomedical Engineering at the New Jersey Institute of Technology, Newark. He currently serves as the director of the Computer Vision Laboratory.

Dr. Shih is currently on the editorial boards of the *International Journal of Pattern Recognition*, the *International Journal of Pattern Recognition Letters*, the *International Journal of Pattern Recognition and Artificial Intelligence*, the *International Journal of Recent Patents on Engineering*, the *International Journal of Recent Patents on Computer Science*, the *International Journal of Internet Protocol Technology*, and the *Journal of Internet Technology*. Dr. Shih has contributed as a steering member, committee member, and session chair for numerous professional conferences and workshops. He was the recipient of the Research Initiation Award from the National Science Foundation in 1991. He won the Honorable Mention Award for Outstanding Paper from the International Pattern Recognition Society and also won the Best Paper Award at the International Symposium on Multimedia Information Processing. He has received several awards for distinguished research at the New Jersey Institute of Technology. He has served several times on the Proposal Review Panel of the National Science Foundation.

Dr. Shih started his mathematical morphology research with applications to image processing, feature extraction, and object representation. His *IEEE Transactions on Pattern Analysis and Machine Intelligence* (*PAMI*) article "Threshold Decomposition of Grayscale Morphology into Binary Morphology" was a breakthrough solution to the bottleneck problem in grayscale morphological processing. His several articles in *IEEE Transactions on Image Processing* and *IEEE Transactions on Signal Processing* were innovations in fast exact Euclidean distance transformation and robust image enhancement and segmentation, using the *recursive soft morphological operators* he developed.

Dr. Shih further advanced the field of solar image processing and feature detection. In cooperation with physics researchers, he has made incredible contributions to bridge in the gap between solar physics and computer science. He and his colleagues have used these innovative computation and information technologies for real-time space weather monitoring and forecasting, and have received over $1 million in National Science Foundation grants. They have developed several methods to automatically detect and characterize filament/prominence eruptions, flares, and coronal mass ejections. These techniques are currently in use at the Big Bear Observatory in California as well as by NASA.

He has made significant contributions to mathematical morphology, pattern recognition, and information hiding, focusing on the security and robustness of digital watermarking and steganography. He has developed several novel methods to

increase embedding capacity, enhance robustness, integrate different watermarking platforms, and break steganalytic systems. His recent article published in *IEEE Transactions on Systems, Man, and Cybernetics* is the first to apply GA-based methodology to breaking steganalytic systems.

Dr. Shih has so far published 130 journal papers, 100 conference papers, and 22 book chapters. The journals in which he has been published are top ranked in the professional societies. He has authored/edited four books: *Digital Watermarking and Steganography*, *Image Processing and Mathematical Morphology*, *Image Processing and Pattern Recognition*, and *Multimedia Security: Watermarking, Steganography, and Forensics*. He has overcome many difficult research problems in multimedia signal processing, pattern recognition, feature extraction, and information security. Some examples are robust information hiding, automatic solar feature classification, optimum feature reduction, fast accurate Euclidean distance transformation, and fully parallel thinning algorithms.

Dr. Shih is a research fellow for the American Biographical Institute and is a senior member of the IEEE. His current research interests include digital watermarking and steganography, digital forensics, image processing, computer vision, sensor networks, pattern recognition, bioinformatics, information security, robotics, fuzzy logic, and neural networks.

1 Introduction

Digital information and data are transmitted more often over the Internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have accelerated the popularity of digital media. Digital images, video, and audio have been revolutionized in the way they can be captured, stored, transmitted, and manipulated. This gives rise to a wide range of applications in education, entertainment, the media, industrial manufacturing, medicine, and the military, among other fields [1].

Computers and networking facilities are becoming less expensive and more widespread. Creative approaches to storing, accessing, and distributing data have generated many benefits for digital multimedia, mainly due to properties such as distortion-free transmission, compact storage, and easy editing. Unfortunately, free-access digital multimedia communication also provides virtually unprecedented opportunities to pirate copyrighted material. Therefore, the idea of using a digital watermark to detect and trace copyright violations has stimulated significant interest among engineers, scientists, lawyers, artists, and publishers, to name a few. As a result, research into the robustness of watermark embedding with respect to compression, image-processing operations, and cryptographic attacks has become very active in recent years, and the developed techniques have grown and been improved a great deal.

In this chapter, we introduce digital watermarking in Section 1.1 and digital steganography in Section 1.2. The differences between watermarking and steganography are given in Section 1.3. Finally, a brief history is described in Section 1.4.

1.1 DIGITAL WATERMARKING

Watermarking is not a new phenomenon. For nearly a thousand years, watermarks on paper have been used to visibly indicate a particular publisher and to discourage counterfeiting in currency. A watermark is a design impressed on a piece of paper during production and used for copyright identification (as illustrated in Figure 1.1). The design may be a pattern, a logo, or some other image. In the modern era, as most data and information are stored and communicated in digital form, proving authenticity plays an increasingly important role. As a result, digital watermarking is a process whereby arbitrary information is encoded into an image in such a way as to be imperceptible to observers.

Digital watermarking has been proposed as a suitable tool for identifying the source, creator, owner, distributor, or authorized consumer of a document or an image. It can also be used to detect a document or an image that has been illegally distributed or modified. Another technology, encryption, is the process of obscuring information to make it unreadable to observers without specific keys or knowledge. This technology is sometimes referred to as *data scrambling*. Watermarking, when

FIGURE 1.1 A paper watermark.

complemented by encryption, can serve a vast number of purposes including copyright protection, broadcast monitoring, and data authentication.

In the digital world, a watermark is a pattern of bits inserted into a digital medium that can identify the creator or authorized users. Digital watermarks—unlike traditional printed, visible watermarks—are designed to be invisible to viewers. The bits embedded into an image are scattered all around to avoid identification or modification. Therefore, a digital watermark must be robust enough to survive detection, compression, and other operations that might be applied to a document.

Figure 1.2 depicts a general digital watermarking system. A watermark message W is embedded into a media message, which is defined as the host image H. The resulting image is the watermarked image H^*. In the embedding process, a secret key K—that is, a random number generator—is sometimes involved to generate a more secure watermark. The watermarked image H^* is then transmitted along a communication channel. The watermark can later be detected or extracted by the recipient.

Imperceptibility, security, capacity, and robustness are among the many aspects of watermark design. The watermarked image must look indistinguishable from the original image; if a watermarking system distorts the host image to the point of being

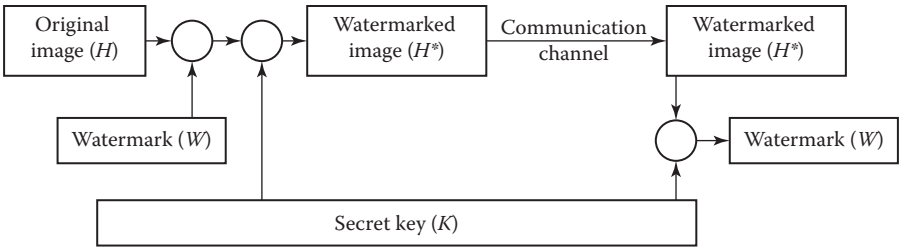

FIGURE 1.2 A general digital watermarking system.

perceptible, it is of no use. An ideal watermarking system should embed a large amount of information perfectly securely, but with no visible degradation to the host image. The embedded watermark should be robust, with invariance to intentional (e.g., noise) or unintentional (e.g., image enhancement, cropping, resizing, or compression) attacks. Many researchers have focused on security and robustness, but rarely on watermarking capacity [2,3]. The amount of data an algorithm can embed in an image has implications for how the watermark can be applied. Indeed, both security and robustness are important because the embedded watermark is expected to be imperceptible and unremovable. Nevertheless, if a large watermark can be embedded into a host image, the process could be useful for many other applications.

Another scheme is the use of keys to generate random sequences during the embedding process. In this scheme, the cover image (i.e., the host image) is not needed during the watermark detection process. It is also a goal that the watermarking system utilizes an asymmetric key, as in public or private key cryptographic systems. A public key is used for image verification and a private key is needed for embedding security features. Knowledge of the public key neither helps compute the private key nor allows the removal of the watermark.

For user-embedding purposes, watermarks can be categorized into three types: *robust*, *semifragile*, and *fragile*. Robust watermarks are designed to withstand arbitrary, malicious attacks such as image scaling, bending, cropping, and lossy compression [4–7]. They are usually used for copyright protection in order to declare rightful ownership. Semifragile watermarks are designed for detecting any unauthorized modifications, while at the same time enabling some image-processing operations [8]. In other words, selective authentication detects illegitimate distortion while ignoring the applications of legitimate distortion. For the purpose of image authentication, fragile watermarks [9–13] are adopted to detect any unauthorized modification at all.

In general, we can embed watermarks in two types of domains: the spatial domain or the frequency domain [14–17]. In the spatial domain we can replace the pixels in the host image with the pixels in the watermark image [7,8]. Note that a sophisticated computer program may easily detect the inserted watermark. In the frequency domain, we can replace the coefficients of a transformed image with the pixels in the watermarked image [19,20]. The frequency domain transformations most commonly used are discrete cosine transform, discrete Fourier transform, and discrete wavelet transform. This kind of embedded watermark is, in general, difficult to detect.

However, its embedding capacity is usually low, since a large amount of data will distort the host image significantly. The watermark must be smaller than the host image; in general, the size of a watermark is one-sixteenth the size of the host image.

1.2 DIGITAL STEGANOGRAPHY

Digital steganography aims at hiding digital information in covert channels so that one can conceal the information and prevent the detection of the hidden message. Steganalysis is the art of discovering the existence of hidden information; as such, steganalytic systems are used to detect whether an image contains a hidden message. By analyzing the various features of stego-images (those containing hidden messages) and cover images (those containing no hidden messages), a steganalytic system is able to detect stego-images. Cryptography is the practice of scrambling a message into an obscured form to prevent others from understanding it, while steganography is the practice of obscuring the message so that it cannot be discovered.

Figure 1.3 depicts a classic steganographic model presented by Simmons [21]. In it, Alice and Bob are planning to escape from jail. All communications between them are monitored by the warden Wendy, so they must hide the messages in other innocuous-looking media (cover objects) in order to obtain each other's stego-objects. The stego-objects are then sent through public channels. Wendy is free to inspect all messages between Alice and Bob in one of two ways: passively or actively. The passive approach involves inspecting the message in order to determine whether it contains a hidden message and then to take proper action. The active approach involves always altering Alice's and Bob's messages even if Wendy may not perceive any traces of hidden meaning. Examples of the active method would be image-processing operations such as lossy compression, quality-factor alteration, format conversion, palette modification, and low-pass filtering.

For digital steganographic systems, the fundamental requirement is that the stego-image be perceptually indistinguishable to the degree that it does not raise suspicion. In other words, the hidden information introduces only slight modifications to the cover object. Most passive wardens detect the stego-images by analyzing their statistical features. In general, steganalytic systems can be categorized into two classes: spatial domain steganalytic systems (SDSSs) and frequency domain steganalytic systems (FDSSs). SDSSs [22,23] are adopted for checking lossless compressed

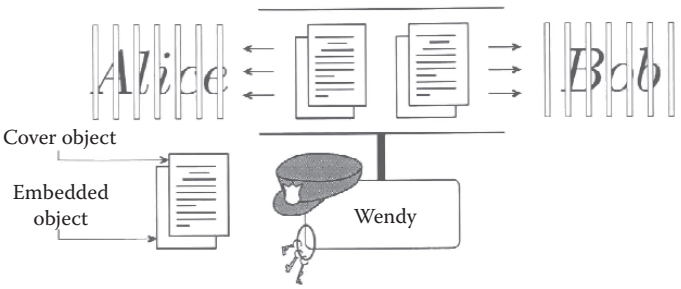

FIGURE 1.3 A classic steganographic model.

images by analyzing the statistical features of the spatial domain. For lossy compressed images, such as JPEG files, FDSSs are used to analyze the statistical features of the frequency domain [24,25]. Westfeld and Pfitzmann have presented two SDSSs based on visual and chi-square attacks [23]. A visual attack uses human eyes to inspect stego-images by checking their lower bit planes, while a chi-square attack can automatically detect the specific characteristics generated by the least-significant-bit steganographic technique.

1.3 DIFFERENCES BETWEEN WATERMARKING AND STEGANOGRAPHY

Watermarking is closely related to steganography; however, there are some differences between the two. Watermarking mainly deals with image authentication, whereas steganography deals with hiding data. Embedded watermarking messages usually pertain to host image information such as copyright, so they are bound with the cover image. Watermarking is often used whenever the cover image is available to users who are aware of the existence of the hidden information and may intend to remove it. Hidden messages in steganography are usually not related to the host image. They are designed to make extremely important information imperceptible to any interceptors.

In watermarking, the embedded information is related to an attribute of the carrier and conveys additional information about or the properties of the carrier. The primary object of the communication channel is the carrier itself. In steganography, the embedded message usually has nothing to do with the carrier, which is simply used as a mechanism to pass the message. The object of the communication channel is the hidden message. As with the application of watermarking, a balance between image perceptual quality and robustness is maintained. Constraints in maintaining image quality tend to reduce the capacity of information embedded. As the application of steganography is different, dealing with covert message transfer, the embedded capacity is often viewed with as much importance as robustness and image quality.

1.4 A BRIEF HISTORY

The term *watermarking* is derived from the history of traditional papermaking. Wet fiber is pressed to expel the water, and the enhanced contrast between the watermarked and nonwatermarked areas of the paper forms a particular pattern and becomes visible.

Watermarking originated in the paper industry in the late Middle Ages—roughly, the thirteenth century. The earliest known usage appears to record the paper brand and the mill that produced it so that authenticity could be clearly recognized. Later, watermarking was used to certify the composition of paper. Nowadays, many countries watermark their paper, currencies, and postage stamps to make counterfeiting more difficult.

The digitization of our world has supplemented traditional watermarking with digital forms. While paper watermarks were originally used to differentiate between

different manufacturers, today's digital watermarks have more widespread uses. Stemming from the legal need to protect the intellectual property of the creator from unauthorized usage, digital watermarking technology attempts to reinforce copyright by embedding a digital message that can identify the creator or the intended recipients. When encryption is broken, watermarking is essentially the technology to protect unencrypted multimedia content.

In 1989, Komatsu and Tominaga proposed digital watermarking to detect illegal copies [26]. They encoded a secret label into a copy using slight modifications to redundant information. When the label matches that of the registered owner, the provider can ensure that the document holder is the same person. As a method, digital watermarking has a long history, but it was only after 1990 that it gained large international interest. Today, a great number of conferences and workshops on this topic are held, and there are a large number of scientific journals on watermarking in publication. This renewed scientific interest in digital watermarking has quickly grabbed the attention of industry. Its widely used applications include copyright protection, labeling, monitoring, tamper proofing, and conditional access.

Watermarking or information embedding is a particular embodiment of steganography. The term *steganography* is derived from the Greek words for "covered or hidden" and "writing." It is intended to hide the information in a medium in such a manner that no one except the anticipated recipient knows the existence of the information. This is in contrast to cryptography, which focuses on making information unreadable to any unauthorized persons.

The history of steganography can be traced back to ancient Greece, where the hidden-message procedure included tattooing a shaved messenger's head, waiting for his hair to grow back, and then sending him out to deliver the message personally; the recipient would then shave the messenger's head once again in order to read the message. Another procedure included etching messages onto wooden tablets and covering them with wax. Various types of steganography and cryptography also thrived in ancient India, and in ancient China, military generals and diplomats hid secret messages on thin sheets of silk or paper. One famous story on the successful revolt of the Han Chinese against the Mongolians during the Yuan dynasty demonstrates a steganographic technique. During the Yuan dynasty (AD 1280–1368), China was ruled by the Mongolians. On the occasion of the Mid-Autumn Festival, the Han people made mooncakes (as cover objects) with a message detailing an attack plan inside (as hidden information). The mooncakes were distributed to members to inform them of the planned revolt, which successfully overthrew the Mongolian regime.

REFERENCES

1. Berghel, H. and O'Gorman, L., Protecting ownership rights through digital watermarking, *IEEE Computer Mag*., 29, 101, 1996.
2. Barni, M. et al., Capacity of the watermark channel: How many bits can be hidden within a digital image?, in *Proc. SPIE*, San Jose, CA, 1999, 437.

3. Shih, F. Y. and Wu, S.Y., Combinational image watermarking in the spatial and frequency domains, *Pattern Recognition*, 36, 969, 2003.
4. Cox, I., et al. Secure spread spectrum watermarking for images audio and video, in *Proc. IEEE Int. Conf. Image Processing*, Lausanne, Switzerland, 1996, 243.
5. Cox, I., et al. Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, 6, 1673, 1997.
6. Lin, S. D. and Chen, C.-F., A robust DCT-based watermarking for copyright protection, *IEEE Trans. Consumer Electronics*, 46, 415, 2000.
7. Nikolaidis, N. and Pitas, I., Robust image watermarking in the spatial domain, *Signal Processing*, 66, 385, 1998.
8. Acharya, U. R. et al., Compact storage of medical image with patient information, *IEEE Trans. Information Technology in Biomedicine*, 5, 320, 2001.
9. Caronni, G., Assuring ownership rights for digital images, in *Proc. Reliable IT Systems*, Vieweg, Germany, 1995, pp. 251–263.
10. Celik, M. et al., Hierarchical watermarking for secure image authentication with localization, *IEEE Trans. Image Processing*, 11, 585, 2002.
11. Pitas, I. and Kaskalis, T., Applying signatures on digital images, in *Proc. IEEE Workshop Nonlinear Signal and Image Processing*, Halkidiki, Greece, 1995, 460.
12. Wolfgang, R. and Delp, E., A watermarking technique for digital imagery: Further studies, in *Proc. Int. Conf. Imaging Science, Systems and Technology*, Las Vegas, NV, 1997.
13. Wong, P. W., A public key watermark for image verification and authentication, in *Proc. IEEE Int. Conf. Image Processing*, Chicago, IL, 1998, 425.
14. Langelaar, G. et al., Watermarking digital image and video data: A state-of-the-art overview, *IEEE Signal Processing Magazine*, 17, 20, 2000.
15. Cox, I. J. et al., Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, 6, 1673, 1997.
16. Petitcolas, F., Anderson, R., and Kuhn, M., Information hiding: A survey, *Proceedings of the IEEE*, 87, 1062, 1999.
17. Cox, I. and Miller M., The first 50 years of electronic watermarking, *J. Applied Signal Processing*, 2, 126, 2002.
18. Bruyndonckx, O., Quisquater, J.-J, and Macq, B., Spatial method for copyright labeling of digital images, in *Proc. IEEE Workshop Nonlinear Signal and Image Processing*, Neos Marmaras, Greece, 1995, 456.
19. Huang, J., Shi, Y. Q., and Shi, Y., Embedding image watermarks in DC components, *IEEE Trans. Circuits and Systems for Video Technology*, 10, 974, 2000.
20. Lin, S. D. and Chen, C.-F., A robust DCT-based watermarking for copyright protection, *IEEE Trans. Consumer Electronics*, 46, 415, 2000.
21. Simmons, G. J., Prisoners' problem and the subliminal channel, in *Proc. Int. Conf. Advances in Cryptology*, Santa Barbara, CA, 1984, 51.
22. Avcibas, I., Memon, N., and Sankur, B., Steganalysis using image quality metrics, *IEEE Trans. Image Processing*, 12, 221, 2003.
23. Westfeld, A. and Pfitzmann, A., Attacks on steganographic systems breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools and some lessons learned, in *Proc. Int. Workshop Information Hiding*, Dresden, Germany, 1999, 61.
24. Farid, H., Detecting steganographic messages in digital images, Technical Report, TR2001-412, Computer Science, Dartmouth College, 2001.
25. Fridrich, J., Goljan, M., and Hogea, D., New methodology for breaking steganographic techniques for JPEGs, in *Proc. SPIE*, Santa Clara, CA, 2003, 143.
26. Komatsu, N. and Tominaga H., A proposal on digital watermark in document image communication and its application to realizing a signature, *Trans. of the Institute of Electronics, Information and Communication Engineers*, J72B-I, 208, 1989.