Chapter 1

Introductory Chapter: Digital Image and Video Watermarking and Steganography

Srinivasan Ramakrishnan

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.84984

1. Overview of watermarking and steganography

Watermarking and steganography are important cryptographic operations on images and videos. Watermarking embeds the ownership symbol in images and videos either visually or invisibly. Steganography hides small piece of information in images and videos invisibly. Watermarking is used mainly for copyright protection, whereas steganography is used to send secret messages. **Table 1** presents the difference between watermarking and steganography.

	Watermarking	**Steganography**
Scope	To provide the ownership	To hide the secret information
Input data	Image or video or multimedia	Any digital data
Secret data	Watermark	Payload
Output data	Watermarked data	Stegodata
Protection	Given to original image	Given to the secret information
Imperceptibility	Required only for invisible watermarking techniques	Highly required
Robustness	Highly required	Desirable
Payload capacity requirement	Moderate	Very high
Challenges	High robustness and good imperceptibility (only for invisible watermark)	Good imperceptibility and high payload capacity

Table 1. Watermarking versus steganography.

2. Applications of watermarking and steganography

Some of the latest applications of the watermarking techniques are (1) copyright protection, (2) digital right management, (3) broadcast monitoring, (4) content integrity, (5) media forensics, (6) fraud and tamper detection, (7) package identification, (8) copy control, (9) user tracking, (10) medical image watermarking, and (11) ownership authentication [1–4].

Similarly, some of the modern use steganography are (1) printer steganography, (2) protection of data alteration, (3) document security, (4) setting of covert channel, (5) distributed steganography, (6) in military, (7) in medical images, (8) online challenge, and (7) corporate espionage [1, 5–8].

3. Challenges in the development of watermarking algorithms

Quality of the watermarking techniques can be accessed through various metrics such as peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), structural similarity index measurement (SSIM), and normalized crosscorrelation (NCC). Most of the real-world application requires good imperceptibility and high robustness. Achieving both of them simultaneously for color images and multimedia documents sought highly efficient watermarking algorithms. Hence, obviously transform domain processing will be the natural choice to meet out these complex requirements.

Fourier transform, discrete cosine transform, radon transform, and wavelet transform are the commonly used transformations for embedding watermarks. Fourier transform provides good resistance against geometric attacks. Discrete cosine transform yields robustness when watermarked images are compressed. Wavelet transform archives good imperceptibility and radon transform can provide good robustness. Though each transform is advantages in its own way, only careful development of watermark embedding and extraction algorithms helps in achieving maximum advantage of the chosen transformation.

Most of these transforms are proving good imperceptibility when some additional decompositions are employed. For example, wavelet transforms and singular value decomposition is the most popular choice. Watermarking techniques should be robust against the following attacks namely (1) cryptographic attacks, (2) removal attacks, (3) protocol attacks, (4) geometric attacks, (5) forgery attacks, (6) low-pass filtering attacks, (7) estimation-based attacks, (8) remodulation attacks, (9) copy attacks, and (10) optimized attacks. Identification of suitable transformation is not only sufficient, but careful development of efficient watermarking algorithms is also required to face these challenges [1–4].

4. Challenges in the development of steganography algorithms

Steganography algorithms can be classified based on the type of data employed as (1) text steganography, (2) image steganography, (3) audio steganography, and (4) video steganography.

http://dx.doi.org/10.5772/intechopen.84984

Some of the commonly used evaluation criteria are invisibility, payload capacity, robustness against image manipulation attacks, and statistical undetectability. Steganalysis can be used to choose good steganography algorithm. Similar to watermarking techniques, steganography algorithms also require careful design and devolvement in order to withstand the following attacks. (1) visual attacks, (2) statistical attacks, (3) histogram attacks, (4) compression attacks, (5) reformat attacks, (6) structural attacks, and (7) subversion attacks [1, 5–8].

5. Conclusion

In this introductory chapter, applications and challenges of both watermarking and steganography are presented. Researchers continue to develop new and efficient watermarking and steganography algorithms. Since huge amount of data are getting digitized, establishing ownership and sharing them secretly are becoming a challenging task. In this book, five interesting algorithms, three for watermarking and two for steganography, are available.

Author details

Srinivasan Ramakrishnan

Address all correspondence to: ram_f77@yahoo.com

Department of Information Technology, Dr. Mahalingam College of Engineering and Technology, India

References

[1] Ramakrishnan S. Cryptographic and Information Security Approaches for Images and Videos. Florida: CRC Press, Taylor & Francis Group; 2018. ISBN: 9781138563841

[2] Zhao X, Ho AT. An introduction to robust transform based image watermarking techniques. In: Intelligent Multimedia Analysis for Security Applications. Berlin, Heidelberg: Springer; 2010. pp. 337-364

[3] Tiwari A, Sharma M. A Survey of transform domain based semifragile watermarking schemes for image authentication. Journal of The Institution of Engineers (India): Series B. 2012;**93**(3):185-191

[4] Khan A, Siddiqa A, Munib S, Malik SA. A recent survey of reversible watermarking techniques. Information Sciences. 2014;**279**:251-272

[5] Fridrich J. Stegnography in Digital Media Principles, Algorithms and Applications. New York: Cambridge University Press; 2010. ISBN: 9780 521 190100

[6] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal Processing. 2010;**90**(3):727-752

[7] Li B, He J, Huang J, Shi YQ. A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing. 2011;**2**(2):142-172

[8] Karampidis K, Kavallieratou E, Papadourakis G. A review of image steganalysis techniques for digital forensics. Journal of Information Security and Applications. 2018; **40**:217-235