Chapter 11
Digital Image Watermarking: Techniques and Emerging Applications

Amit Kumar Singh  
Jaypee University of Information Technology, India

Basant Kumar  
Motilal Nehru National Institute of Technology, India

Mayank Dave  
NIT Kurukshetra, India

Satya Prakash Ghrera  
Jaypee University of Information Technology, India

Anand Mohan  
IIT (BHU), India

ABSTRACT

Recently, with the explosive growth of Information and Communication Technologies (ICT), various new opportunities emerged for the creation and delivery of content in digital form which includes applications such as real time video and audio delivery, electronic advertising, digital libraries and web publishing. However, these advantages have the consequent risks of data piracy, which motivate towards development of new protection mechanisms. One such effort that has been attracting interest is based on digital watermarking techniques. This chapter discusses the basic concepts of digital watermarking techniques, performances parameters and its potential applications in various fields. In this chapter, we also discuss various spatial and transform domain techniques and compare the performance of some reported wavelet based watermarking techniques. Finally, the latest applications of watermarking techniques have been discussed. This chapter will be more important for researchers to implement effective watermarking method.

1. INTRODUCTION

The growth of information technology in the recent years has led to the creation and delivery of content in digital such as real-time video and audio delivery, electronic advertising, digital libraries and web publishing. On the darker side, this form of information had the consequent risks of increased data piracy. Therefore need to develop methods to safeguard and secure these means become a necessity. Techniques such as digital watermarking are gaining popularity to serve for this purpose. Digital watermarking is a technique for inserting information, also known as watermark, into an image, which can be later extracted.
or detected for variety of purposes including identification and authentication. In addition to providing security, this technique can also be used to recognize the source, owner, distributor or creator of a document or an image. Simmons was imagine a sample scenario where watermarking can be thought of in terms of the “Prisoner’s Problem” (Simmons, 1984).

It suggests that Alice and Bob are arrested for some crime and are sent in two different cells as shown in Figure 1. A warden named Wendy has arbitrated all communications between them which acts as a hindrance to their escape plan. If any suspicious communication is detected by the warden she will inhibit the exchange of all messages and place them in solitary confinement. So both parties must communicate invisibly in order to arouse the warden suspicion. In this situation, one person creates a picture of blue cow lying on a green meadow and sends this piece of art to another person. Warden has no any idea that the color of the objects in the picture and easily transmit the information to other person.

Data hiding is the art of hiding data into cover message without any perceptual distortion of the cover message for the purpose of identification, annotation and copyright. Here, different conditions may occur to affect this process (Bender et al., 1996): 1) How much data to be hidden 2) the need for invariance of these data under the conditions where a cover message is subjected to distortion and 3) the degree to which the data must be immune to interception, modification or removal by the third one. Data hiding techniques are classified in to two categories steganography and digital watermarking (Katzenbeisser & Petitcolas, 2000). The former refers to hiding of a secret message inside another message in order to avoid others to detect or decode it. It is used for spying in corporate and intelligence industries like for copyright purposes in entertainment industry. However, digital watermarking is a technique where a data called watermark is embedded into a host signal (image, audio, video or a text document) robustly and invisibly at the same time (Armstrong & Yetsko, 2004). Steganography and Watermarking can be classified from each other in the following ways:

- The watermarking systems are restricted only to hide the information of a digital object whereas Steganographic systems can be used to hide any information.
- Steganography aim for imperceptibility in human senses whereas digital watermarking aim tries to control the robustness is the top priority.
- Communication in watermarking systems is usually one to many while that in steganography is usually between a sender and a receiver i.e. point to point.
Related Content

Digital Image Steganography: Survey, Analysis, and Application
[www.igi-global.com/chapter/digital-image-steganography/244924?camid=4v1a](www.igi-global.com/chapter/digital-image-steganography/244924?camid=4v1a)

Towards the Integration of Blockchain and IoT for Security Challenges in IoT: A Review

Recent Developments in Cryptography: A Survey
[www.igi-global.com/chapter/recent-developments-in-cryptography/188509?camid=4v1a](www.igi-global.com/chapter/recent-developments-in-cryptography/188509?camid=4v1a)

A Review of Cryptographic Algorithms for the Internet of Things
[www.igi-global.com/chapter/a-review-of-cryptographic-algorithms-for-the-internet-of-things/222271?camid=4v1a](www.igi-global.com/chapter/a-review-of-cryptographic-algorithms-for-the-internet-of-things/222271?camid=4v1a)