Chapter IX
Visibility Control and Quality Assessment of Watermarking and Data Hiding Algorithms

Patrick Le Callet
Polytech'Nantes, University of Nantes, IRCCyN Lab, France

Florent Autrusseau
Polytech'Nantes, University of Nantes, IRCCyN Lab, France

Patrizio Campisi
Università degli Studi Roma TRE, Italy

ABSTRACT

In watermarking and data hiding context, it may be very useful to have methods checking the invisibility of the inserted data or at least, checking the objective quality after the mark embedding or after an attack on the watermarked media. Many works exist in the literature dealing with quality assessment mainly focused on compression application. Nevertheless, visual quality assessment should include special requirements that depend on the application context. This chapter presents an extended review of both subjective and objective quality assessment of images and video in the field of watermarking and data hiding applications.

INTRODUCTION

In the past few years, there has been an explosion in the use and distribution of digital multimedia data, essentially driven by the diffusion of the Internet. In this scenario, watermarking techniques have been devised to answer the ever-growing need to protect the intellectual property (copyright) of digital still images, video sequences, or audio from piracy attacks in a networked environment like the World Wide Web. Although copyright protection was the very first application of watermarking, different uses have been recently proposed in literature. Fingerprinting, copy control, broad-

cast monitoring, data authentication, multimedia indexing, content-based retrieval applications, medical imaging applications, covert communication (steganography), and error concealment, (Barni & Bartolini, 2004; Doerr & Dugelay, 2003; Kundur, Su, & Hatzinakos, 2004) are only a few of the new applications where watermarking can be usefully employed. Moreover, digital watermarking has been recently used for quality assessment purposes (Campisi, Carli, Giunta, & Neri, 2003; Ninassi, Le Callet, & Autrusseau, 2006), as well as for improved data compression (Campisi, Kundur, Hatzinakos, & Neri, 2002; Campisi & Piva, 2006).

Roughly speaking data hiding is the general process by which a discrete information stream is merged within media content. The general watermark embedding procedure consists of embedding a watermark sequence, which is usually binary, into host data by means of a key. In the detection/extraction phase, the key is used to verify either the presence of the embedded sequence or to extract the embedded mark. When considering a watermarking scheme, depending on its specific application, different requirements need to be achieved. One of them is the *perceptual invisibility* of the superimposed mark onto the host data. This implies that the alterations caused by the watermark embedding into the data should not degrade their perceptual quality. Moreover, when these techniques are used to preserve the copyright ownership with the purpose of avoiding unauthorized data duplications, the embedded watermark should be detectable. This is required even if malicious attacks or non-deliberate modifications (i.e., filtering, compression, etc.) affect the embedded watermark. This requirement is known as watermark *security*. When the watermark is required to be resistant only to non-malicious manipulations the watermarking techniques is referred to as *robust*. For some applications, when the robustness requirement is severely required, each attempt of removing the mark should result in irreversible data quality degradation. As a consequence the quality of the image must noticeably decrease before the removal attempt succeeds. However in some applications the host data are intended to undergo a limited number of signal processing operations. Therefore we talk about *semi-fragile* watermarking when the watermark needs to be robust only to a limited number of set of manipulations, while leaving the perceived quality of the host data intact. On the contrary, when unwanted modifications of the watermarked data affect even the extracted watermark, the embedding scheme is known as *fragile*. Fragile watermarking can be used to obtain information about the tampering process. In fact, it indicates whether or not the data has been altered and supplies localization information as to where the data was altered. *Capacity* is another watermarking requirement, referring to the number of bits of information that can be embedded in the original data, which needs to be fulfilled, depending on the specific application. These requirements conflict each other. Therefore the optimal trade-off is strictly tied to the target application.

A comprehensive review of the different needed requirements depending on the intended application is given in Fridrich (1999) and they are summarized in Table 1 where a score from 1 to 7 indicating in increasing order the level of importance of the specific requirement is specified for a class of applications.

Because of the proliferation of watermarking algorithms and their applications, some benchmarks (Michiels & Macq, 2006; Pereira, Voloshynovskiy, Madueno, Marchand-Maillet, & Pun, 2001; Petitcolas, Anderson, & Kuhn, 1998) have been proposed in order to allow a fair comparison among watermarking algorithms in terms of robustness against various attacks. However, no equal attention has been devoted to the proposition of benchmarks tailored to assess the watermark perceptual transparency or, equivalently, to perform the watermarked image quality assessment. Thus, the mean square error (MSE) or the peak