Chapter 10
Hardware Implementations of Image/Video Watermarking Algorithms

Fayez M. Idris
German-Jordanian University, Jordan

ABSTRACT

Digital watermarking is a process in which a secondary pattern or signature, called a watermark, is hidden into a digital media (e.g., image and video) such that it can be detected or extracted later for different intentions. Digital watermarking has many applications including copyright protection, authentication, tamper detection, and embedding of electronic patient records in medical images. Various software implementations of digital watermarking algorithms can be built. While software implementations can address digital watermarking in off-line applications, they cannot meet the requirements of many applications. For example, in consumer electronic devices, a software solution would be very expensive. This has motivated the development of hardware implementations of digital watermarking. In this chapter, the authors present a detailed survey of existing hardware implementations of image and video watermarking algorithms. Fundamental design issues are discussed and special techniques exploited to enhance efficiency are identified. Future outlooks are also presented to address the challenges of hardware architecture design for image and video watermarking.

INTRODUCTION

The proliferation of the World Wide Web and advances in digital technologies have led to the widespread of digital media (text, audio, image, and video). This has allowed the development of new services and business models, which has a profound effect on our social, political, and economical lives. We have become better connected (any where any time) over recent years. On our desktops, laptops, or personal digital assistants (PDAs), we have the potential of accessing and reaching numerous resources to communicate, do business, learn, or have fun. However, the availability of digital content which can be easily duplicated, manipulated, and widely redistributed

DOI: 10.4018/978-1-4666-2136-7.ch010

has given birth to large-scale piracy. Illegal piracy of copyrighted content may cause financial loss and cause many legal issues. Therefore issues such as authentication, tamper detection, and copyright protection are becoming increasingly important. Although many laws and regulations exist for protecting intellectual property, complementary technical measures are needed.

Protection of analogue content has been based on binding the content and its physical medium. Mass reproduction of analogue content is not feasible because it is time-consuming and generates a loss of quality. In comparison to analogue data, manipulation of digital data is simpler and more flexible, reproduction results in perfect copies and mass distribution is very feasible. A non-experienced user, for example, can make perfect duplicate of digital media and change its content using inexpensive or freely distributed tools and applications. Moreover, digital media can be easily made available to millions of people through boundless distribution systems such as e-mails and the Internet. This may result in infringement of copyrights, where the owners lose control after releasing their copyrighted content for distribution.

Two technological techniques have been used to protect digital content. We note that each technique has a different goal. The first is based on preventing illegal users from accessing the content. A physical blockade may be used to prohibit a user from reading the bits that represent the content. For example, a proprietary format enables the detection of a copied medium and prevents access to the media stored on it. The second is based on cryptography, where digital media is changed into incomprehensible form. Encryption allows accessing the media, but it prevents accessing the meaning of their semantics, a secret key is required to convert the media to intelligible form. However, once the content is decrypted, it is unprotected. In addition, devices must be compliant with certain standards and mechanisms to protect decryption keys are required (Maes, Kalker, Linnartz, Talstra, Depover, & Haitsma, 2000).

Physical blockade and encryption provide good protection as long as the content is in digital form. Once the digital media is converted to analogue in order to play or view it, it can be recorded and digitized. This is known as the "digital hole" and it is a major source of illegal duplication and redistribution (Deskshare, 2005). Digital watermarking is considered a promising technique to solve the "digital hole" problem and the most prominent technologies in forensic Digital Rights Management (DRM) (Böhle, Rader, Weber, & Weber, 2008). Digital watermarking basically consists of hiding a pattern or a message, called the watermark, into digital media in an imperceptible way. A detection algorithm can retrieve the watermark. Unlike the first two methods, in watermarking a general user is allowed to access the content but cannot claim the ownership. A watermark serves many purposes. For example, a watermark could hold the identity of the copyright owner or copy control information.

In digital watermarking algorithms, the computational complexity per pixel is low, but the computations have to be performed at image/video rate (Maes, Kalker, Linnartz, Talstra, Depover, & Haitsma, 2000). The video rates ranges from 352×240 pixels at 30 frames/sec for VCD to 4096×2034 pixels at 30 frames/sec for HDTV (Deskshare, 2005; Wiegand, Sullivan, Bjontegaard, & Luthra, 2003). Hence, digital watermarking algorithms are compute intensive necessitating the use of special purpose architecture for real time implementations. Recently, special purpose architectures that implement image/video watermarking have been reported in the literature. This chapter presents a detailed survey of hardware implementations of image and video watermarking algorithms.

The rest of this chapter is organized as follows. To start with, an overview of image and video watermarking is presented and general requirements for different applications are briefly discussed. Then, the design issues and implementation challenges in image and video watermarking are discussed with emphasis on computational