Chapter XVI
Efficient Transparent JPEG2000 Encryption

Dominik Engel
University of Salzburg, Austria

Thomas Stütz
University of Salzburg, Austria

Andreas Uhl
University of Salzburg, Austria

ABSTRACT

In this chapter we investigate two different techniques for transparent/perceptual encryption of JPEG2000 files or bitstreams in the context of digital rights management (DRM) schemes. These methods are efficient in the sense of minimizing the computational costs of encryption. A classical bitstream-based approach employing format-compliant encryption of packet body data is compared to a compression-integrated technique that uses the concept of secret transform domains, in our case a wavelet packet transform.

INTRODUCTION

Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the application requirements for a particular multimedia environment (Uhl & Pommer, 2005).

For example, real-time encryption of visual data using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level (e.g., TV news broadcasting [Macq & Quisquater, 1995]). In this context, several selective or partial encryption schemes have been proposed recently which do not strive for maximum security, but trade off security for computational complexity by restricting the encryption to the perceptually most relevant parts of the data.

However, encryption may have an entirely different aim as opposed to pure confidentiality in the context of multimedia applications. Macq and Quisquater (1994, 1995) introduce the term *transparent encryption* mainly in the context of digital TV broadcasting: A broadcaster of pay TV does not always intend to prevent unauthorized viewers from receiving and watching his program, but rather intends to promote a contract with nonpaying watchers. This can be facilitated by providing a low quality version of the broadcasted program for everyone; only legitimate (paying) users get access to the full quality visual data. This is meant also by the term *try and buy* scenario. Therefore, privacy is not the primary concern in such an environment. The simplest approach to achieve this would be to simply distribute both versions, a low quality version to all potential viewers, and a high quality version only to paying viewers. However, this is mostly not desired due to the excessive demand of storage and bandwidth.

Transparent encryption usually transmits a high quality version of the visual data to all possible viewers but aims at protecting the details of the data which enable a pleasant viewing experience in an efficient manner. If these data are missing (i.e., are encrypted), the user is (hopefully) motivated to pay for the rest of the data which may be accessed upon transmission of the required key material by the broadcaster. Another application area of transparent encryption is preview images in image and video databases. Therefore, there are two major requirements that have to be met concurrently:

- To hide a specific amount of image information (security requirement)
- To show a specific amount of image information (quality requirement)

While the first requirement is a generalization of the confidentiality encryption approach—the condition of full encryption of all image information is extended to a *specific amount*—the second requirement, namely to explicitly demand a certain image quality, is completely different from scenarios where confidentiality or privacy are the primary aims.

To implement transparent encryption, Macq and Quisquater (1995) propose using line permutations in the transform domain of a lossless multi-resolution transform. The permutations are only applied in the region of the transform domain corresponding to fine grained details of the data. Droogenbroeck and Benedett (2002) propose encrypting bitplanes of the binary representation of raw image data, in contrast to the privacy-focused approach they suggest to start with the LSB bitplane. With respect to JPEG encoded images, the authors suggest to encrypt sign and magnitude bits of medium and high frequency discrete cosine transform (DCT) coefficients (note that this is again exactly just the other way round as compared to encrypting low frequency coefficients only for privacy protection [Cheng & Li, 1996; Kunkelmann, 1998]). Droogenbroeck (2004) extends this latter idea to *multiple encryption* where different sets of DCT coefficients are encrypted by different content owners, and *over encryption*, where these sets do not have an empty intersection (i.e., coefficients are encrypted twice or even more often). Bodo, Laurent, & Dugelay (2003) propose a technique called *waterscrambling* where they embed a watermark into the motion vectors of an MPEG stream, thereby reducing the video quality significantly—only a legitimate user has access to the key and may descramble the motion vectors.

Transparent encryption may be implemented in the simplest way in the context of scalable or embedded bitstreams since parsing the file and searching for the data to be protected can be avoided to a large extent in this setting. Transparent encryption is achieved in this environment by simply encrypting the enhancement layer(s). This has been proposed by Kunkelmann and Horn using a scalable video codec based on a