Chapter III
Digital Watermarking in the Transform Domain with Emphasis on SVD

Maria Calagna
Dipartimento di Informatica, Universita' di Roma La Sapienza, Italy

ABSTRACT

The chapter illustrates watermarking based on the transform domain. It argues that transform-based watermarking is robust to possible attacks and imperceptible with respect to the quality of the multimedia file we would like to protect. Among those transforms commonly used in communications, we emphasize the use of singular value decomposition (SVD) for digital watermarking. The main advantage of this choice is flexibility of application. In fact, SVD may be applied in several fields where data are organized as matrices, including multimedia and communications.We present a robust SVD-based watermarking scheme for images. According to the detection steps, the watermark can be determined univocally, while other related works present flaws in watermark detection. A case study of our approach refers to the protection of geographical and spatial data in case of the raster representation model of maps.

INTRODUCTION

In recent years digital watermarking has been applied to cope with the main problems of digital spreading of multimedia files: copyright protection, copy protection, proof of ownership, and transaction tracking. *Copyright protection* concerns the possibility to identify the intellectual property on a specific object that could be publicly available to external users. *Copy protection* concerns the prevention of re-distribution of illegal copies of protected objects. This issue is afforded

by the adoption of compliant players and compliant recorders; while the former ones are able to play only protected content, the other ones can refuse to create new copies of some content, in the case this action is considered as illegal.

The *proof of ownership* can be used in a court of law in order to assess the ownership rights related to objects. Finally, *transaction tracking* is an emergent research area that is aimed to prevent illegal use of protected objects, by taking into account each transaction event in the digital chain: play, copy, distribution, sale, and so on. In this context, a proper solution to trace user actions is fingerprinting, a process that embeds a distinct watermark in each distributed object.

Watermarking is a technical solution that can be used to address the issue of intellectual rights protection through the embedding of information (watermark) into digital objects (cover). The watermark is a binary string; when it is associated to the cover, it identifies the content univocally. Watermark presence can be identified through detection and extraction procedures that depend on the embedding technique. Multimedia files, including images, video files, and audio files are some examples of possible covers. According to the real-world scenario, watermarking may be classified as *fragile* or *robust*. In a fragile watermarking system the embedded watermark is sensible to changes, then, fragile systems are used for tamper detection. State-of-the-art algorithms are able to identify if changes occur in a digital object and at which locations they occur. On the converse, in a robust watermarking system, the watermark is resistant to class of attacks and the application of stronger ones could destroy the watermark and make the digital content unusable, as well. Definitely, distinguishing properties of watermarking are:

- Imperceptibility
- Robustness

Imperceptibility is related to the quality of the watermarked file. Quality is acceptable if the distortion due to the embedded message is irrelevant for the real-world applications. For example, some broadcast transmissions have poor levels of quality, then the embedded secret message may be imperceptible, even if there are further channel degradations.

The *peak-to-signal-noise-ratio* (PSNR) is a common metric for the difference of quality between two possible images or videos, based on the mean squared error (MSE).

Given two images I_1 and I_2, both of $M \times N$ pixels, the MSE is given by:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I_1(i,j) - I_2(i,j)] \qquad (1)$$

and the PSNR is computed as:

$$PSNR = 20\log\left(\frac{M\_Intensity}{RMSE}\right) \qquad (2)$$

with *M_Intensity* indicating the maximum intensity value in the images and RMSE indicating the squared root of MSE. $I_k(i,j)$ represents the intensity of pixel *(i, j)* in the *k*-th image. The higher the PSNR value between the cover and the watermarked object is, the better the quality the watermarked file is. This metrics give an idea of the quality difference between two images or videos, so the relative values are more relevant than the absolute ones. Thus, by applying the PSNR value, we can consider how the quality difference between two images changes according to the watermarking system in use, or according to the size of the embedded watermark or, alternatively, according to the watermark strength.

The quality level of the watermarked file may be sacrificed for a stronger constraint on the robust-