Chapter VII
Statistical Watermark Detection in the Transform Domain for Digital Images

Fouad Khelifi
The Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, UK

Fatih Kurugollu
The Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, UK

Ahmed Bouridane
The Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, UK

ABSTRACT

The problem of multiplicative watermark detection in digital images can be viewed as a binary decision where the observation is the possibility that watermarked samples can be thought of as a noisy environment in which a desirable signal, called watermark, may exist. In this chapter, we investigate the optimum watermark detection from the viewpoint of decision theory. Different transform domains are considered with generalized noise models. We study the effect of the watermark strength on both the detector performance and the imperceptibility of the host image. Also, the robustness issue is addressed while considering a number of commonly used attacks.

INTRODUCTION

Recently, we have seen an unprecedented advance in the use and distribution of digital multimedia data. However, illegal digital copying and forgery have become increasingly menacing as the duplication means are easy to use. This makes the protection of copyrighted original copies from illegal use and unrestricted broadcasting a very challenging task. These challenges and issues have involved the field of watermarking for the

Figure 1. Multi-bit watermark extraction system

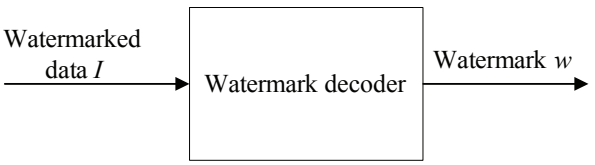
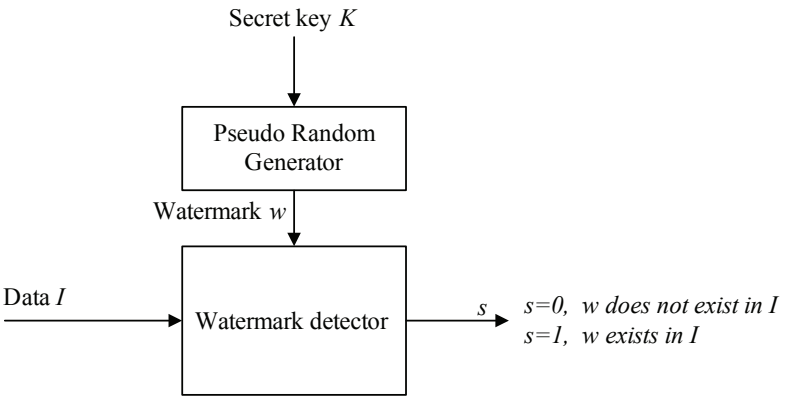


Figure 2. One-bit watermark detection system



protection and security of digital data (Arnold, Schmucker, & Wolthusen, 2003).

Watermarking is the embedding of a hidden secondary data into the host data within an embedding distortion level. The robustness requires that the watermark information must be decoded/detected even if the watermarked data has undergone additional distortions. Existing systems are divided in two groups depending on the roles that watermarks play. In the first group, the watermarks are viewed as transmitted multi-bit information, where the decoder extracts the full version of the embedded message bit by bit. In such a case, the decoder already assumes that the input data is watermarked (Figure 1).

In the second group, known as one-bit watermarking, the watermarks serve as verification codes, as such a full decoding is not really necessary. It is used to decide whether or not a particular message or pattern is present in the host data (Figure 2).

In practice, the security of the entire one-bit watermarking systems is ensured by using a secret key, as commonly employed in communications, which is required to generate the watermark sequence. Only the legal owner of the watermarked data knows the key for the generation of that watermark and proves his/her ownership.

Depending on the embedding rule used in a watermarking system, the watermark is often additive or multiplicative (Langelaar, Setyawan, & Langendijk, 2000). To get better performances in terms of robustness and imperceptibility, both are used in the transform domain (Barni, Bartolini, Cappellini, & Piva, 1998; Cheng & Huang, 2001a). In fact, the energy compaction property exhibited in the transform domain suggests that the distortions introduced by a hidden data into a number of transform coefficients will be spread over all components in the spatial domain so as the change of the pixels values is less significant.

In additive watermarking, the watermark is simply added to a set of transformed coefficients