# Chapter 35
# Commutative Watermarking-Encryption of Multimedia Data Based on Histograms

**Roland Schmitz**
*Stuttgart Media University, Germany*

**Shujun Li**
*University of Kent, UK*

**Christos Grecos**
*Central Washington University, USA*

**Xinpeng Zhang**
*Shanghai University, China*

## ABSTRACT

*Histogram-based watermarking schemes are invariant to pixel permutations and can thus be combined with permutation-based ciphers to form a commutative watermarking-encryption scheme. In this chapter, the authors demonstrate the feasibility of this approach for audio data and still image data. Typical histogram-based watermarking schemes based on comparison of histogram bins are prone to desynchronization attacks, where the whole histogram is shifted by a certain amount. These kind of attacks can be avoided by synchronizing the embedding and detection processes, using the mean of the histogram as a calibration point. The resulting watermarking scheme is resistant to three common types of shifts of the histogram, while the advantages of previous histogram-based schemes, especially commutativity of watermarking and permutation-based encryption, are preserved. The authors also report on the results of testing robustness of the still image watermark against JPEG and JPEG2000 compression and on the possibility of using histogram-based watermarks for authenticating the content of an image.*

DOI: 10.4018/978-1-7998-7705-9.ch035

## INTRODUCTION

Encryption and watermarking are both important tools in protecting digital contents, e.g. in digital rights management (DRM) systems. While encryption is used to protect the contents from unauthorized access, watermarking can be deployed for various purposes, ranging from ensuring authenticity of content to embedding metadata, e.g. copyright or authorship information, into the contents. Heterogeneous end-to-end media distribution scenarios, where the ultimate receiver of the media data may be unknown to the sender, call for protection schemes in which both watermarking and encryption need to be combined in a flexible way.

The concept of commutative watermarking-encryption (CWE) was first discussed in (Herrera-Joancomarti et al., 2005) with a special emphasis on watermarking in the encrypted domain. Four properties about watermarking in the encrypted domain are formulated in Sec. 2.2 of Herrera-Joancomarti et al.'s report:

**Property 1:** The marking function $M$ can be performed in the encrypted domain.
**Property 2:** The verification function $V$ is able to reconstruct a mark in the encrypted domain when it has been embedded in the encrypted domain.
**Property 3:** The verification function $V$ is able to reconstruct a mark in the encrypted domain when it has been embedded in the clear domain.
**Property 4:** The decryption function does not affect the integrity of the watermark.

All four properties should hold without the marking and verification functions having access to the encryption key, and without the encryption and decryption functions having access to the watermarking key. The four properties can be fulfilled in the most natural way if the encryption operation and the watermarking operation commute, meaning that the outcome is the same no matter whether the encrypted media are watermarked or if the watermarked media are encrypted (see also Sec. 4).

In this chapter, histogram-based watermarking schemes which are capable of being integrated into a CWE scheme are described. For still images, it is well known that histogram-based watermarking schemes are resistant to permutations of image pixels. In particular, using histograms implies robustness against rotation, scaling and translation (RST) of images. In (Schmitz, 2012) this fact has been utilized to devise a commutative watermarking-encryption (CWE) scheme by choosing a permutation cipher for encryption and a histogram-based scheme for watermarking.

In (Schmitz & Gruber, 2017) it has been demonstrated that the basic approach also works for audio data. Here, the permutation cipher is applied to discrete sample values obtained from sampling the analogous audio signal. Likewise, the histogram is computed from the amplitude values of the sample values.

Typical histogram-based watermarking schemes like those proposed in (Schmitz et al., 2012) and (Chrysochos et al., 2007) work by comparing selected histogram bins, where the selection process is controlled by a watermarking key. If the whole histogram is shifted by a small amount, i.e. by adding a small number to each pixel value, the detector will use completely different bin pairs for extracting the embedded watermark and will produce wrong results. To overcome this problem, a synchronization process between embedder and detector is employed that is based on the global mean of the histogram.

The rest of the chapter is organized as follows. In Sec. 2 previous approaches to CWE along with other histogram-based watermarking algorithms are briefly summarized. Section 3 describes three types of histogram shifts which may be used to attack histogram-based watermarking algorithms. Sec.