Towards Robust Invariant Commutative Watermarking-Encryption Based on Image Histograms

Roland Schmitz, Stuttgart Media University, Stuttgart, Germany
Shujun Li, University of Surrey, Guildford, UK
Christos Grecos, Independent Imaging Consultant, Glasgow, UK
Xinpeng Zhang, Shanghai University, Shanghai, China

ABSTRACT

Invariant Commutative Watermarking-Encryption means to use a cipher that does not have any impact on a certain feature space, which can thus be used for embedding watermarks either before or after encryption. For example, histogram-based watermarking schemes are invariant to pixel permutations and can be combined with permutation-based ciphers to form a Commutative Watermarking-Encryption (CWE) scheme. However, typical histogram-based watermarking schemes based on comparison of histogram bins are prone to de-synchronization attacks, where the whole histogram is shifted by a certain amount. In this paper the authors investigate the possibility to avoid this kind of attacks 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 scheme against JPEG and JPEG2000 compression.

Keywords: Commutative Watermarking-Encryption (CWE), De-Synchronization Attacks, Histogram-Based Watermarking, Image Histogram, Permutation-Based Encryption

1. 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

DOI: 10.4018/ijmdem.2014100103
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. 4.4).

The present paper is mainly concerned with a histogram-based watermarking scheme that is capable of being integrated into a CWE scheme. 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.

However, 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, in the present paper, we further improve our earlier work described in (Schmitz et al., 2012) by deploying a synchronization process between embedder and detector that is based on the global mean of the histogram. A preliminary edition of the present paper was presented at the 2013 IEEE International Symposium on Multimedia (ISM), see (Schmitz et al., 2013).

The rest of the paper is organized as follows. In Sec. 2 we briefly summarize previous approaches to CWE along with other histogram-based watermarking algorithms. Section 3 describes the three types of histogram shifts we have investigated, and Sec. 4 describes the proposed algorithm in greater detail. In Sec. 5 we discuss experimental results for the algorithm, especially its robustness against histogram shifts and lossy compression. In Sec. 6 we provide a qualitative comparison between the watermarking scheme proposed in the present paper and previous histogram-based schemes. Section 7 concludes the paper and gives directions for further work.

2. RELATED WORK

2.1. Commutative Watermarking-Encryption (CWE)

While encryption algorithms are evaluated mainly according to their security and run-time performance, in watermarking there are more and often conflicting requirements (Cox et al., 2007): Watermarking security normally refers
Improved Illumination Independent Moving Object Detection Algorithm Applied to Infrared Video Sequences
www.igi-global.com/chapter/improved-illumination-independent-moving-object-detection-algorithm-applied-to-infrared-video-sequences/94125?camid=4v1a

A Review on 3D Signing Avatars: Benefits, Uses and Challenges
Kabil Jaballah and Mohamed Jemni (2013). International Journal of Multimedia Data Engineering and Management (pp. 21-45).
www.igi-global.com/article/a-review-on-3d-signing-avatars/78746?camid=4v1a

Games and Simulations: A New Approach in Education?
www.igi-global.com/chapter/games-simulations-new-approach-education/49379?camid=4v1a