Chapter VI
Securing and Protecting the Copyright of Digital Video Through Watermarking Technologies

Evanthia Tsilichristou
University of Patras, Greece

Spiridon Likothanasis
University of Patras, Greece

ABSTRACT

The basic principle of watermarking is the addition of the watermark signal to the host data that we wish to watermark. The addition is taking place in a way that the watermark signal is discreet and secure among the rest signals. Its retrieval, either partial or complete from the rest of signals, must be also possible only by using a secret key. In this chapter, we are going to deal with the digital video watermarking. First, we will name its applications, requirements, and the most important trends, then we will describe some of the most significant techniques of the specific process.

INTRODUCTION

Digital video watermarking techniques and algorithms offer a great support to real world digital video applications. These applications include the copy control, the broadcast monitoring, the fingerprinting, the video authentication, the copyright protection as well as the enhanced video coding.

Nowadays, the copying of a digital video is very simple by using a recorder. For this reason, a watermark is embedded to the digital video so that its copying through unauthorized recorders may not be possible. If the recorder is able to read the hidden information comprised into the watermark, then it is authorized to produce copies, otherwise it must not carry out the copying.
Securing and Protecting Copyright of Digital Video Through Watermarking Technologies

As to the broadcast monitoring, the aim of the watermarking is the determination of the identity of the video object transmitted. The owners having the right to create a video want to secure their privileges any time their property is broadcasted. The principal idea here embeds identification information (a unique watermark) into the data, which is identified by a computer. This identification information is obtained directly and with reliability after the decoding process.

In fingerprinting, the aim of the watermark is to show which user created the illegal copies. The problem arises when a ‘traitor’ spares the protected material without having any sort of permission on behalf of the holder of the right on intellectual property. In order to solve the problem, the basic idea is to be able to identify the identity of the traitor when detecting an illegal copy so that we can prosecute him in court. This can happen by embedding into data an indelible and invisible watermark which determines the client’s identity.

The authentication techniques are useful for confirming that a video content is the original. Different methods for the verification of the video content authenticity as well as for the protection against falsification are proposed. Researchers have also studied the use of digital watermarking aiming at verifying the integrity of the digital video content. A basic technique is the typical embodiment of a timestamp into the video frames. The result of the aforementioned technique is that the detection of alterations may be possible.

REQUIREMENTS OF VIDEO WATERMARKING

A video watermarking technique must fulfil some requirements. We mention below the three most principal requirements for video watermarking. The first is that the technique above should be robust to non-hostile video processing. The second is that it should be robust to collusions and the third one is that it should be performed in real-time.

The robustness of the digital watermarking is always estimated in regard to the survival of the watermark after the implementation of the attacks. In the environment of digital watermarking the future value of attacks that take place in the video is multiple. Many different, non-hostile attacks in video are in fact likely to happen. The term non-hostile refers to those attacks where for example, the provider of the content processes a bit of information from his digital data for the most efficient handling of his sources. Afterwards, we name any procedures that can lead to non-hostile attacks: the addition of noise during the transmission through a wireless network, the conversion of a digital to analog or analog to digital signal, the gamma correction in order to increase the contrast, the changes across display formats (4/3, 16/9, 2.11/1), the changes of spatial resolution (NTSC, PAL, SECAM), the attack by a handheld camera, the changes in frame rate, the video editing process (cut-and-splice or cut-insert-splice) and the overlay with a chart (logos and labels).

Another basic requirement is the robustness against collusions. The term collusion refers to all hostile users who unite their knowledge, for example the watermarked data they have in order to produce illegally the non-watermarked ones. There are two types of collusion: the type I collusion and the type II collusion. The same watermark is embedded into different copies of different data. The type I collusion estimates the watermark of every watermarked data. Then, it combines in a linear way the watermarks estimated and provides an exact estimation of it; for example, it measures the mean of various evaluations. Since the collusion obtained a good estimation of the watermark, it removes it from the rest and in this way we have the non-watermarked data. When different watermarks are embedded into different copies of
Related Content

Investigating B-to-B Social Media Implementation: E-Marketing Orientation and Media Richness Perspective
Ying Kai Liao, Candice Chang and Giang Nu To Truong (2020). *Journal of Electronic Commerce in Organizations* (pp. 18-35).
[www.igi-global.com/article/investigating-b-to-b-social-media-implementation/241246?camid=4v1a](www.igi-global.com/article/investigating-b-to-b-social-media-implementation/241246?camid=4v1a)

Mobile E-Commerce on Mobile Phones
[www.igi-global.com/chapter/mobile-commerce-mobile-phones/4871?camid=4v1a](www.igi-global.com/chapter/mobile-commerce-mobile-phones/4871?camid=4v1a)

A Review of Platforms for Digital Goods
[www.igi-global.com/chapter/a-review-of-platforms-for-digital-goods/149006?camid=4v1a](www.igi-global.com/chapter/a-review-of-platforms-for-digital-goods/149006?camid=4v1a)

Development and Testing of an E-Commerce Web Site Evaluation Model
[www.igi-global.com/chapter/development-testing-commerce-web-site/39668?camid=4v1a](www.igi-global.com/chapter/development-testing-commerce-web-site/39668?camid=4v1a)