

Chapter 30

Two Spatial Watermarking Techniques for Digital Images

Dumitru Dan Burdescu
University of Craiova, Romania

Liana Stănescu
University of Craiova, Romania

Marian Cristian Mihăescu
University of Craiova, Romania

ABSTRACT

The rapid growth of digital multimedia technologies brings tremendous attention to the field of digital authentication. Digital watermarking has become widely recognized as an effective measure for copyright protection of multimedia data. The owner or the distributor of the digital images can insert a unique watermark into copies for different customers or receivers, which will be helpful to identify the source of illegal copies. In this chapter the authors present two original spatial authentication techniques for digital images. These new algorithms yield an invisible watermark that is robust to various kinds of attacks. The main principle is the utilization of a virtual (2D or 3D) graph embedded into the digital images. Then, the colors of some vertices of the virtual graph are slightly modified for obtaining the watermark. The proposed techniques modify pixels or voxels of the object by a spatial watermark insertion scheme. These techniques can be used for all kinds of digital images, color or black and white, and the new algorithms produce an invisible robust watermark. The techniques lower the computational complexity that normally rises with the traditional watermarking algorithms. This approach reduces computation and implementation complexity of the algorithms. These techniques seem to replace advantages of the transform domain techniques with those of the spatial domain techniques.

INTRODUCTION

Multimedia content is vulnerable to large scale copying and redistribution through easily accessible networks. Unauthorized digital copying is a major concern for multimedia content providers.

In many contexts it is essential to be able to tell if a message is authentic or if it has been modified by an adversary. This applies for instance to forensic photography, where someone may want to forge or disable evidence, by doctoring an image. The most well-established solutions are cryptographic techniques such as digital signatures or message authentication codes (MAC). These solutions are mature and widely trusted. The signature or the MAC is transmitted together with the message, and the receiver can verify that the message fits the MAC or signature. While an adversary can modify the message, it is computationally infeasible to generate a matching MAC or signature. Unfortunately after decrypting, this method fails to any type of duplication or image retransmission.

Alternative solutions have been proposed in digital watermarking. This new emerging technology, digital watermarking, provides a promising way to protect a digital image from illicit copying and manipulating.

Digital watermarking is a method to hide some information that is integrated with a multimedia object (Sequeira and Kundur 2001). The object may be any form of multimedia, such as image, audio, video, or text. A digital watermark is an invisible signal that is embedded directly in the digital media (images, audio, video, 3D objects, etc.) so that it is inseparable from the digital media.

Digital watermarking, in general, allows us to embed a message (watermark) within another data file (such as an image) called the host. The embedding is done by imperceptible changes to the host, so that the watermarked host can replace the original for all practical purposes. A basic application of watermarking is to extend a legacy data structure. There are (Cox et al. 2007) presented two advantages of digital watermarking for authenti-

cation. Firstly, the authentication information is hidden as an inherent part of the message (host). Therefore it can be incorporated in a legacy data structure. Thus it avoids the appended signature of cryptology. The other advantage is more subtle. Because the watermark is hidden in the data, it will undergo the same transformations as the data. By observing the transformed watermark, it may be possible to determine the exact transformation the message has undergone, and possibly undo it.

The two most common methods used for digital image watermarking are spatial and spectral domain methods (Bassali et al. 2000, Mukherjee et al. 2004). Spectral domain methods have several advantages over the spatial domain methods. First, they are more robust, since the watermark is inserted in the perceptually significant parts of the image, which corresponds to the mid-frequency range. Second, they are well-suited to resist the compression attacks. Third, some transform domain algorithms are robust against specific geometric transformations such as Discrete Fourier Transform (DFT) which is robust to most affine transformations. Although transform domain algorithms have more advantages in providing robustness, sometimes it is difficult to satisfy imperceptibility constraints in the spatial domain simultaneously with the spectral domain constraints.

In order to take full advantage of both the spatial and the spectral domains, researchers started looking at the joint time-frequency representation of the image, which gives a more comprehensive representation of the image compared to looking at each domain individually (Barkat et al. 2003). This approach also provides flexibility in the amount of data that can be hidden inside an image (Zheng et al. 2007).

Watermarking of 3D meshes has received a limited attention due to the difficulties encountered in extending the algorithms developed for 1D (audio) and 2D (images and video) signals to topological complex objects such as meshes. Other difficulties arise from the wide variety of

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/two-spatial-watermarking-techniques-digital/70997

Related Content

The New Digital Wave of Rationalization: A Loss of Autonomy

Lambèr Royakkers and Rinie van Est (2020). *International Journal of Technoethics* (pp. 59-74).

www.irma-international.org/article/the-new-digital-wave-of-rationalization/258848

Research Ethics Among Undergraduates of the Social Sciences

Shazia Shahab Shaikhand Abdulrazaque Chhachhar (2024). *Methodologies and Ethics for Social Sciences Research* (pp. 184-200).

www.irma-international.org/chapter/research-ethics-among-undergraduates-of-the-social-sciences/337056

Blind Watermarking of Three-Dimensional Meshes: Review, Recent Advances and Future Opportunities

Kai Wang, Guillaume Lavoué, Florence Denis and Atilla Baskurt (2013). *Digital Rights Management: Concepts, Methodologies, Tools, and Applications* (pp. 1559-1585).

www.irma-international.org/chapter/blind-watermarking-three-dimensional-meshes/71046

Robotics, Ethics, and the Environment

Jason Borenstein (2012). *International Journal of Technoethics* (pp. 17-29).

www.irma-international.org/article/robotics-ethics-environment/67363

Infosphere to Ethosphere: Moral Mediators in the Nonviolent Transformation of Self and World

Jeffrey Benjamin White (2011). *International Journal of Technoethics* (pp. 53-70).

www.irma-international.org/article/infosphere-ethosphere-moral-mediators-nonviolent/62309