

Copyright Protection through Digital Watermarking

Farook Sattar

Nanyang Technological University, Singapore

Dan Yu

Nanyang Technological University, Singapore

INTRODUCTION

Today, the Internet is a worldwide broadcasting capability, a mechanism for information dissemination and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. With the rapid evolution of digital networks, digital libraries and World Wide Web (WWW) services, the convenient broadcasting or exposition of digital products on the global network leads easily to illegal copying, modifying and retransmission. The Internet has spawned many copyright issues involving multimedia content distribution. Let's say an owner would like to sell or distribute a work to legal/registered users only. If the work were subsequently copied/redistributed illegally, how could the owner find who was responsible?

Cryptographic techniques provide an effective solution for securing the delivery process and controlling the use of the contents that an user has obtained. However, with flawless transmission through the network, the contents after decryption are exactly the same as the original data. The contents can be copied perfectly infinite times. A user can also manipulate the contents. Digital watermarking (Arnold, Schmucker, & Wolthusen, 2003; Katzenbeisser & Petitcolas, 2000) offers a way to counter copyright piracy on global networks that are not solvable by cryptography. It provides proof and tracking capabilities to illegal copying and distribution of multimedia information.

Most existing digital watermarking schemes are based on some assumptions for watermark detection and extraction. Some schemes require the previous knowledge of watermark locations, strengths or some thresholds. In some algorithms, the watermark is estimated with the help of the original watermark information. To ensure the robustness and invisibility of the watermark, the optimum embedding locations are usually different for different images. For a large image database, it could be a disadvantage to require watermark location and strength information for watermark

detection and extraction. A large amount of information then needs to be stored. On the Internet, an owner would like to distribute multimedia data by signing different watermarks to different users in order to prevent illegal redistribution of the data by a legal user. In this scenario, watermark detection and extraction algorithms requiring information of either watermark embedding locations and strengths or the original watermark should fail, since one does not know exactly which watermark is embedded in a particular copy of the watermarked image.

To this end, we present a new blind watermarking scheme (Yu, Sattar, & Ma, 2002; Yu & Sattar, 2003, 2005) based on Independent Component Analysis (ICA) (Hyvarinen, 1999; Hyvärinen & Oja, 1999; Lee, 1998) for color images, which can overcome existing problems of watermark detection and extraction as described above. The new ICA-based scheme is found to be efficient in the application of data tracking/tracing for multimedia distribution through the Internet against other digital watermarking schemes. By adopting this ICA-based watermarking scheme, an efficient multimedia distribution framework/protocol for copyright protection can be accomplished.

This article is organized as follows: The watermark embedding and extraction algorithms for color image watermarking using the new ICA-based scheme are presented next, followed by a discussion and comments on the results, security issues, summary and future works.

WATERMARKING SCHEME FOR COLOR IMAGES

Watermark Embedding Scheme for Color Images

First, we offer an overview of the proposed watermark embedding scheme for color images, followed by watermark generation and the watermark embedding

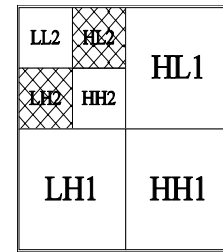
scheme. Then we present the issues of channel selection for color image embedding and side information needed for verification/identification of the recipient/user.

Overview of Color Image Watermarking Scheme

A flowchart for the color image watermark embedding scheme is shown in Figure 1. Assume the original image, I , is in RGB color space. First, we have to transform the color image into selected color space. The watermark embedding can use one channel of the selected color space or all of them. Tradeoffs exist by embedding one or all of the channels. By embedding all three channels, the robustness of a watermark can be improved in terms of detection and extraction, while the visual quality of the watermarked image may be easily degraded unless the human visual masking function is properly used. In this article, we illustrate the proposed ICA-based watermarking scheme by embedding only one channel, C . The watermark is inserted into the selected channel adaptively according to the embedding algorithm shown in Figure 1. This is achieved by maintaining the watermarked image quality; for example, its PSNR measure is within a pre-defined range of 40-50 dB, while tuning the parameter of watermark embedding strength. The final watermarked color image, denoted as I' , is obtained by inverting the marked channel, C' , together with the other two unmarked channels back to the RGB color space.

The Y channel (i.e., the luminance component) of the color image in YUV color space is selected for water-

Figure 2. Second-level wavelet decomposition of Y component for a color image

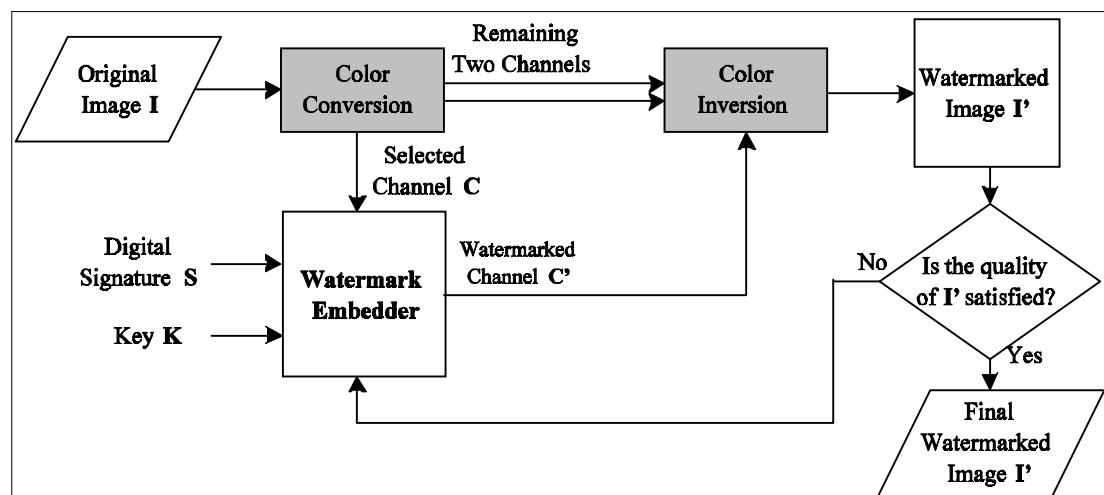


mark embedding. Figure 2 shows a second-level wavelet decomposition of the Y component into four bands—low frequency band (LL), high frequency band (HH), low-high frequency band (LH), and high-low frequency band (HL). The watermark embedding for the two sub-bands (e.g., LH2, HL2 of the second-level wavelet decomposition) containing the middle frequencies, will be demonstrated in the following section.

Color Watermarked Image: An Example

Some digital signature/pattern or company logo (S), for example, a text image can be used to generate the watermark (W). The noise visibility function (NVF)-based (Voloshynovskiy, Herrigel, Baumgaertner & Pun, 1999) visual mask is then generated to identify the suitable embedding locations; that is, the highly textured and edge regions. The original color Lena image

Figure 1. The flowchart of the adaptive watermark embedding scheme for color images



5 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/copyright-protection-through-digital-watermarking/18046

Related Content

GLARE: An Open Source Augmented Reality Platform for Location-Based Content Delivery

Enrico Gandolfi, Richard E. Ferdig, David Carlyn, Annette Kratcoski, Jason Dunfee, David Hassler, James Blank, Chris Lenartand Robert Clements (2021). *International Journal of Virtual and Augmented Reality* (pp. 1-19).

www.irma-international.org/article/glare/290043

Sixth Sense Technology: Advances in HCI as We Approach 2020

Zeenat AlKassimand Nader Mohamed (2017). *International Journal of Virtual and Augmented Reality* (pp. 18-41).

www.irma-international.org/article/sixth-sense-technology/188479

REVERIE Virtual Hangout: An Immersive Social and Collaborative VR Experience

Ioannis Dourmanisand Daphne Economou (2021). *International Journal of Virtual and Augmented Reality* (pp. 18-39).

www.irma-international.org/article/reverie-virtual-hangout/298984

Changes in Online Subjectivity: Artificial Users, Subject Fragmentarization, and Multimodal Interaction

Zdenek Smutnyand Vaclav Janoscik (2019). *Intimacy and Developing Personal Relationships in the Virtual World* (pp. 1-20).

www.irma-international.org/chapter/changes-in-online-subjectivity/207915

N-SAFE: A Neuro-Secure Framework for Metaverse and Future Intelligent Environments

Jorge A. Ruiz-Vanoye, Ocotlán Díaz-Parra, Jaime Aguilar-Ortiz, Francisco R. Trejo-Macotellaand Eric Simancas-Acevedo (2027). *Next-Generation Security Frameworks for the Metaverse* (pp. 161-198).

www.irma-international.org/chapter/n-safe/413513