J. Vis. Commun. Image R. 20 (2009) 323–338

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

A visible watermarking algorithm based on the content and contrast aware (COCOA) technique

Min-Jen Tsai *

National Chiao Tung University, Institute of Information Management, 1001 Ta-Hsueh Road, Hsin-Chu 300, Taiwan, ROC

ARTICLE INFO

Article history:
Received 13 June 2008
Accepted 31 March 2009
Available online 17 April 2009

Keywords:
CSF
Human Vision System
NVF
Visible watermarking
Wavelet transform
Copyright protection
Image inpainting
Image recovery

ABSTRACT

A novel visible watermarking algorithm based on the content and contrast aware (COCOA) technique with the consideration of Human Visual System (HVS) model is presented in this study. In order to determine the optimal watermark locations and strength at the watermark embedding stage, the COCOA visible watermarking utilizes the global and local characteristics of the host and watermark images in the discrete wavelet transform (DWT) domain. To achieve the best tradeoff between the embedding energy of watermark and the perceptual translucence, the utilization of contrast–sensitive function, noise visible function of perceptual model, and the basis function amplitudes of DWT coefficients are fine tuned, for the best quality of perceptual translucence and noise reduction of the COCOA algorithm. The experimental results demonstrate that COCOA technique not only provides high PSNR values for the watermarked images, but also preserves the watermark visibility under various signal processing operations, especially the watermark removal attack.

1. Introduction

Due to the advancement of digital technologies and rapid communication network deployment, a wide variety of multimedia contents have been digitalized and their distribution or duplication made easy without any reduction in quality through both authorized and unauthorized distribution channels. With the advantages of easy editing and reproduction of digitalized data, the protection of the intellectual rights and the authentication of digital multimedia no doubt have become issues of great importance in recent years.

Over the last two decades, software, multimedia, and all digital content-driven industries, whether on the Internet or not, have also come to rely on effective copyright protection, especially as a revolution is underway in digital entertainment and marketing. In the beginning, conventional encryption algorithms such as DES or RSA are directly adopted to protect digital media. In these cryptographic systems, only the valid users who have the correct decryption key can decrypt the encrypted content and use it. But once such content is decrypted and the users can duplicate or retransmit it repeatedly, the authors will have no way to track those digital data. Therefore, conventional cryptography is evidently not a good way to solve this problem.

Digital watermarking [1] has been extensively researched and regarded as a potentially effective means for protecting copyright of digital media in recent years, since it makes possible the embedding of secret information in the digital content to identify the copyright owner. Digital watermarking describes methods and technologies that allow hidden information, for example, a sequence of numbers or recognizable pattern in digital media, such as images, video and audio. Many different digital watermarking techniques have been proposed by a number of researchers, and these methods can be divided into various categories [2]. One important classification is to divide digital watermarking algorithms into visible and invisible ones according to the perceptivity of watermark data in watermarked contents. Since the visible watermarking schemes protect copyrights in a more active method, they not only prevent pirating but also recognize the copyright of multimedia data immediately. Digital contents embedded with visible watermarks will overlay recognizable but unobtrusive copyright patterns to identify its ownership. Therefore, a useful visible watermarking technique should retain all details of the contents, while ensuring that the embedded patterns are difficult or even impossible to be removed, so that no one could use watermarked data illegally. Thus this study will mainly focus on the research for visible watermarking techniques.

Regarding the digital watermarking techniques, Fig. 1(a) and (b) describes the generic structure for watermark embedding and extraction processes. First, a host image (original image) directly embeds watermark in spatial domain or is transformed into frequency domain through the well-known spread spectrum approach, i.e. DFT (discrete Fourier transform), DCT (discrete

* Fax: +1 886 3 572 3792.
E-mail addresses: mjtsai@cc.nctu.edu.tw, mjtsai@gmail.com.

1047-3203/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jvcir.2009.03.011

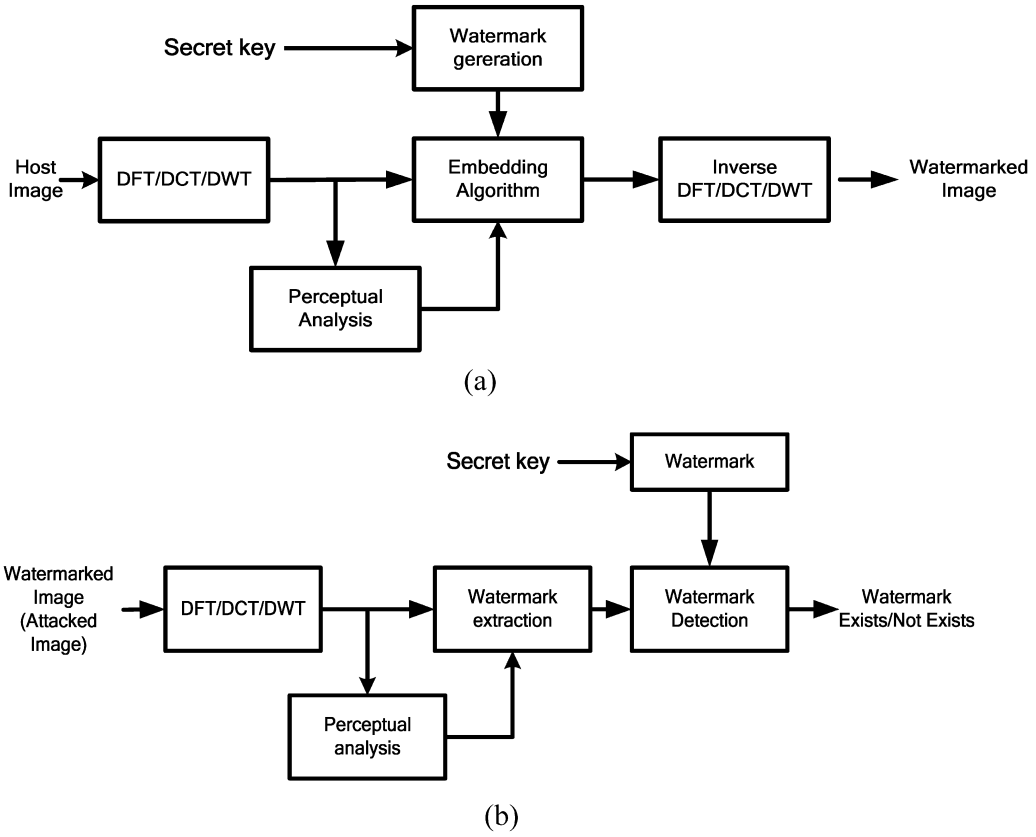

Fig. 1. (a) Watermark embedding process. (b) Watermark extraction process.

cosine transform) or DWT (discrete wavelet transform). However, the algorithms using transform domain approach develop more robust watermarking techniques than directly embedding watermark into the spatial domain. Consequently, coefficients are passed through a perceptual analysis block that determines how strong the watermark in embedding algorithm can be, so that the resulting watermarked image is acceptable. The secret key is applied to generate watermark and watermark embedding location. The watermark is embedded through using a well-designed algorithm based on mathematical or statistical model. If the host image is employed in frequency domain, the inverse spread spectrum approach is then adopted to obtain a watermarked image [1]. The watermark extraction applies to the similar operations in embedding processes. It employs the inverse operations or uses the mathematical or statistical characteristic to extract the embedded watermark. Watermark detection decides whether an image has been watermarked and if the watermark exists or not by calculating the correlation between the embedded watermark and the extracted one.

The goal of this paper is to propose a novel scheme for the copyright protection of colour images by using the visible watermark called COCOA. This visible watermarking algorithm is based on content and contrast aware (COCOA) with the Human Visible System (HVS) model to get the best trade-off between the embedding energy of the watermark and the perceptual translucence for a visible watermark. The rest of this paper is organized as follows. Related works about visible watermarking will be introduced briefly in Section 2. The details of the COCOA algorithm will be explained in Sections 3 and 4 will show the experimental results with discussion in Section 5, and the conclusion is in Section 6, respectively.

2. Related works

Digital contents embedded with visible watermarks will overlay recognizable but unobtrusive copyright patterns to identify its ownership. Therefore, a visible watermarking technique should remain details of the contents and ensure embedded patterns difficult or even impossible to be removed, and no one could use watermarked data illegally. An effective visible watermarking algorithm usually requires meeting a set of requirements [3,4]. These requirements include:

- The watermark in the marked digital contents should be obvious and recognizable to any person having normal or corrected visual accommodation, even if that person is color-blind. Clearly, the visible watermark should be visible in both color and monochrome images.
- It should be possible to adjust the strength of embedding applied to the digital contents by referring its characteristics of the digital contents, so that the watermark could be made as obtrusive or unobtrusive as desired without introducing any other artifacts. It should not only protect the digital contents from unauthorized uses but also prevent it from being so unattractive that no one is interested in viewing it.
- The patterns of the watermark in the embedded contents should be visible, and should form a recognizable symbol to identify content owners or providers.
- All details of the unmarked digital contents should be preserved in the marked digital ones. It means that corresponding pixel values in marked regions between the original and watermarked digital contents should be different in brightness, but the same in hue and saturation.