IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB7277

Chapter XIII

Embedding Robust Gray-Level Watermark in an Image Using Discrete Cosine Transformation

Chwei-Shyong Tsai and Chin-Chen Chang
National Chung Cheng University, Taiwan, ROC

Tung-Shou Chen and Ming-Huang Chen
National Taichung Institute of Technology, Taiwan, R.O.C.

Digital watermarking is an effective technique to protect the intellectual property rights of digital images. In general, a gray-level image can provide more perceptual information; moreover, the size of each pixel in the gray-level image is bigger. Commonly, gray-level digital watermarks are more robust. In this chapter, the proposed watermarking scheme adopts a gray-level image as the watermark. In addition, discrete cosine transformation (DCT) technique and quantization method are applied to strengthen the robustness of the watermarking system. Both original image and digital watermark, processed by DCT transformation, can build a quantization table to reduce the information size of the digital watermark. After quantized watermark is embedded into the middle frequency bands of the transformed original image, the quality of the watermarked image is always visually acceptable because of the effectiveness of the quantization technique. The experimental results show that the embedded watermark can resist image cropping, JPEG lossy compression, and destructive processes such as image blurring and sharpening.

This chapter appears in the book, Distributed Multimedia Databases: Techniques and Applications by Timothy K. Shih.

INTRODUCTION

Nowadays, along with rapid development of international network, information can be attained more conveniently, which, however, directly suggests that people may surf the network as well as download the necessary digital data between blinks. Unfortunately, this convenience also exists with a great disadvantage: digital data are open to the weakness of free distribution, unauthorized copy or distortion for personal modification without warning. To be specific, the legal owner of the digital data is consequently financially damaged.

How to protect the intellectual property of the digital data is a significant issue to discuss. Digital watermarking techniques, most widely used at present to secure digital images, have been already proven effective for their established value in many publications.

Through digital image watermarking techniques, a signal – a so-called watermark – can be embedded into the original digital image. The watermark, used as a logo, a mark, or even a serial number, can provide sufficient protection against any illegal copyright invasion. Basically, digital image watermarking techniques include watermark embedding process and watermark extracting process. The embedding process goes first to embed a watermark into the original digital image for generating a watermarked image. For better security of the embedded position, secret keys will be selected. The legal owner, as expected, may feel relieved to circulate his or her watermarked image in the network. In case the copyright is challenged, the embedded watermark can be immediately extracted to verify the authority. During this verification, an arbitrator will be required as the third party, to whom a time-stamped secret key has already been registered by the owner. The evidence of time-stamped secret key, undoubtedly, shields the security of copyright.

On the ground of related works (Bender, Gruhl, Morimoto and Lu,1996; Bors and Pitas, 1996; Chang, Chen and Chung, 2001; Chang and Hwang, 2001; Chang and Tsai, 2000; Chang and Wu, 2000; Cox, Kilian, Leighton and Shamoon, 1997; Cox and Linnartz, 1998; Craver, Memon, Yeo and Yeung,1998; Hsu and Wu, 1999; Hwang, Chang and Hwang, 1999; Kutter, Jordan and Bossen,1998; Niu, Lu and Sun, 2000; Swason, Kobayashi and Tewfik, 1998) digital image watermarking techniques must be responsible for the following six prerequisites:

1) Imperceptibility: in the watermarked image, the embedded watermark must be invisible to the eye.
2) Un-detection: any illegal user who tries to detect the entrance of the watermark through other techniques such as statistical analysis will find that it is impossible.
3) Un-deletion: for illegal users, it will be a herculean task trying to delete the embedded watermark.
4) Robustness: the embedded watermark must be "sticky" enough to refuse any distortion coming from compression, or destruction of any size or manner.
5) Extraction without original image: without the necessity to keep the original copy right image, more storage space can be saved.
6) Real-time processing: embedding and extracting watermark must satisfy the condition of speed in use.

Digital watermarking technology as known goes through the fields of spatial domain and frequency domain. Spatial domain is strong in its swift computation, but soft in resisting information destruction. Frequency domain, although in need of considerable computation to transform data, stands firm to guard the information processing without the fear of being distorted or destroyed. In terms of data transformation, Fourier transformation, discrete cosine transformation (DCT), and wavelet transformation are frequently used.