Distortion caused by DCT-based image compression techniques on spatial-domain watermark

Vo Hao Tu  
Faculty of Information Technology  
University of Technology, Sydney, Australia  
vohao@it.uts.edu.au

Tom Hintz  
Faculty of Information Technology  
University of Technology, Sydney, Australia  
hintz@it.uts.edu.au

Abstract The ease of duplication and distribution of multimedia data, leads to the protection and copyright issue. Digital watermarks have been considered to address this growing concern. A watermark can be a sequence of bits representing a serial number, a logo or picture, and is directly adhered to the original host. A variety of watermarking techniques have been reported. Such techniques can be broadly classified in two categories: spatial-domain and transform-domain based.

In this paper, we will concentrate on watermarking of still images, which is the case that has generated the largest amount of research in the field, we will address the distortion caused by the spatial-domain based watermarking technique, with a watermark embedded across the eight different bit planes of a 8-bit greyscale image pixel values, and the distortion caused by the DCT-based image compression technique on the embedded watermark stated above, at typical compression factors.

Keywords: Copyright protection, image processing, digital watermark, spatial-domain, human visual system, discrete cosine transform, compression techniques.

1 Introduction

With the rapid growth of multimedia data, which are readily manipulated, duplicated, and distributed widely over the Internet, the protection and enforcement of intellectual property rights for digital media has become an important issue.

Cryptography is an effective solution to the digital distribution problem, but it has to be coupled with costly and specialized hardware in order to preclude direct access to data in digital format. However, most cryptographic protocols are concerned with secure communications instead of altering copyright infringements [1].

A more effective solution to alleviate this protection and ownership rights problem is to use invisible digital watermarking scheme, which refers to the embedding of secret messages, unobtrusive marks or labels that can be represented as bits into the digital multimedia [2].

Unlike encryption, which does not provide a way to examine the original data in its protected form, the watermark does prevent a user from listening to, viewing, examining, or manipulating the content.

Watermarking is the direct embedding of additional information into the original host. The hidden copyright information is encoded into digital data by making small modifications to the data samples, e.g., pixels.

Ideally, there should be no perceptible difference between the watermark and the original host and the watermark should be difficult to remove or alter without damaging the host. In particular, the watermark should be robust against common image processing operations, like resizing, cropping, filtering, dithering, etc., and common image compression techniques [3].

Several watermarking techniques have been proposed. One uses a checksum on the image data which is embedded in the least significant bit of certain pixels [4]. Others add a maximum length linear shift register sequence to the pixel data and identify the watermark by computing the spatial cross correlation function of the sequence and the watermarked image [5].

Transparent watermarking techniques can be fragile, robust, or semi-fragile. Placing the watermark information into the perceptually insignificant portions of the host data guarantees imperceptibility and provides fragile marking capabilities. For a watermarking technique to be robust, the watermark should be embedded in the perceptually significant portion of the host data [6].

Current work on watermarking falls into two broad categories: source-based and destination-based schemes. Source-based schemes focus on ownership identification/authentication. Destination-based schemes focus on tracing the end-user in the case of illegal use such as reselling [7].

Applications for digital watermarking include copyright protection, fingerprinting, authentication, copy control, tamper detection, and data hiding applications such as broadcast monitoring.

2 Watermarking Processes

2.1 Encoding Process

For greyscale or colour-image watermarking, watermark embedding techniques are designed to insert the watermark directly into the original host, such as the luminance or color components or into some transformed version of the original data to take advantage of perceptual properties or robustness to particular signal