International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **3(B)**, March **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 1401–1410

A SIMPLE DIGITAL WATERMARKING BY THE ADAPTIVE BIT-LABELING SCHEME

Ching-Yu Yang[1], Wu-Chih Hu[1], Wei-Ying Hwang[2] and Ya-Fen Cheng[2]

[1]Department of Computer Science and Information Engineering
National Penghu University
No. 300, Liu-Ho Rd., Magong, Penghu 880, Taiwan
{ chingyu; wchu }@npu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chi Nan University
No. 1, University Rd., Puli, Nantou County 54561, Taiwan
{ s97321536; s97321529 }@ncnu.edu.tw

Received February 2009; revised June 2009

Abstract. *Based on integer wavelet transform (IWT), this study proposes a novel data hiding technique via the adaptive bit-labeling scheme. The proposed method includes bit-marking, modulus-2, and coefficient-bias steps. More specifically, a small (primary) watermark is first embedded in the three high subbands of the L1 IWT by bit-marking as well as in the L2 and L3 IWT by modulus-2. A large message, which is also known as the secondary watermark, is then hidden in the high subbands of the L1 IWT using the coefficient-bias. To promote robustness performance, instead of hiding bits directly in the blocks, the authors use an adaptive bit-labeling scheme to a block, which could correctly signify the hidden bits at the receiver. Simulations show that the primary watermark hidden in stego-images generated by the proposed method are robust against manipulations such as JPEG2000, JPEG, cropping, (color) quantization, noise additions, low-pass filtering, (edge) sharpening, brightness, contrast, winding and inverting. Experiments also confirm that under the condition of attacking-free the secondary watermark can be successfully extracted by the decoder. Moreover, the perceived quality of the resulting images is good.*

Keywords: IWT-based watermarking, Adaptive bit-labeling scheme

1. **Introduction.** In today's technology environment, people often use their network access, including asymmetrical digital subscriber line (ADSL), cable modem, fiber-to-the-home (FTTH), or worldwide interoperability for microwave access (WiMAX), to distribute and share resources on the Internet. However, data can be eavesdropped, grabbed, illegally tampered with or falsified during transmission. To address this risk, data hiding techniques can achieve the goals of copyright protection, proof of ownership or content authentication. Generally speaking, data hiding techniques [1,2] are roughly divided into two categories: fragile watermarking and robust watermarking. Fragile watermarking techniques are designed to conceal a message in a host media and hopefully not attract the attention of adversaries. The merits of these techniques [3-7] are providing a large hiding capacity and maintaining a good resultant perceived quality. However, message extraction can fail if even a slight alteration occurs in the stego-images. To resist intentional (or unintentional) manipulations, many authors [8-14] developed robust watermarking methods to solve this issue. Wang and Pearmain [10] recommended two watermarking techniques based on relative modulation of the pixel value (in the spatial domain) and the DCT coefficient value (in the transform domain), respectively. The spatial technique