International Journal of Innovative Computing, Information and Control
Volume **5**, Number **7**, July **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 1911–1917

A DC-BASED APPROACH TO ROBUST WATERMARKING WITH HAMMING-CODE

Mong-Fong Horng[1], Bo-Cheng Huang[2], Ming-Han Lee[3] and Yau-Hwang Kuo[2]

[1]Department of Electronic Engineering
National Kaohsiung University of Applied Sciences
415, Chien Kung Road, Kaohsiung, Taiwan
mfhorng@ieee.org

[2]Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan

[3]Department of Computer Science and Information Engineering
Shu-Te University
Kaohsiung, Taiwan

Received March 2008; revised July 2008

Abstract. *In the past decade, watermarking technology had been recognized as a significant security technique to protect valuable digital contents. However, the robustness against possible attacks, including codec, is concerned by many researchers. In this paper, a DC-based approach to robust watermarking is proposed. Although classical watermarking schemes had been widely developed in frequency-domain hide information, hidden information usually is corrupted and damaged by ordinary codec operations. The lack of robustness against possible codec attack is an important issue of advanced watermarking technique. In this study, we find the polarity of DC components in each image block is robust to the DCT/IDCT operations. Thus, a new watermarking scheme based DC-component is developed. In this proposed scheme, information bits are encoded and hidden in the DC-components of each image block. The experimental results indicate that (1) hidden information can be recovered from compression/decompression attacks and (2) the information-hiding process is low computation-complexity. Besides, the relationship between block size and the amount of hidden information is also investigated to illustrate the deployment strategy in real applications.*

1. **Introduction.** In recent years, as the high-speed networking technology evolving, a variety of information services is presented and causes huge amount of information transportation between hosts. Thus, digital images could be more easily duplicated and distributed. The protection of digital information had become one of significant and critical issues in digital content technology. In the past, information-hiding technologies were proposed [1-6] to insert some secret information into the protected digital contents. The secret information inserted in content is regards as a watermark to indicate the ownership of protected contents. Generally, such a watermark can be either visible or invisible to offer various applications, for examples, the determination of content ownership and the encryption of critical data in ordinary image contents.

The watermarking for ownership identification is the focus of this investigation. Typical features of an ideal ownership-identifying watermarking should include (1) Imperceptibility, (2) Robustness and (3) Unambiguity. In other words, the embedded watermark should