International Journal of Innovative Computing, Information and Control
Volume **2**, Number **4**, August **2006**

ICIC International ©2006 ISSN 1349-4198
pp. **841–848**

COUNTERFEITING ATTACKS ON TWO ROBUST WATERMARKING SCHEMES

Zhe-Ming Lu and Xin-Wu Liao

Visual Information Analysis and Processing Research Center
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen 518055, P. R. China
zhemingl@yahoo.com; liaoxinwu@dsp.hit.edu.cn

Received May 2005; revised October 2005

Abstract. *In this paper, we present two attacking methods aiming at two robust watermarking schemes respectively. It is shown that these two robust watermarking schemes have some security problems and are vulnerable to the counterfeiting attack. Specifically, given a watermarked image, one can make a statistical analysis on it to estimate the key parameters used for watermark insertion and forge the corresponding watermark into another image without knowing the secret key and even without explicitly knowing the watermark. In the simulation experiment, we successfully implement the attacks on these two robust watermarking schemes and demonstrate the effectiveness of the proposed counterfeiting attacking schemes.*
Keywords: Robust watermark, Counterfeiting attack, Dither modulation

1. **Introduction.** With the further development of multimedia technologies and the rapid spread of computer networks, the copyright protection and the authentication of digital contents have been the two most serious problems. Digital watermarking is now drawing the attention as a new method of solving these two problems. Digital watermarking is the technique which embeds some special information to the digital multimedia such as images, audio and video, without being perceived by human beings. Watermarking schemes can be classified as either robust or fragile. Robust watermarks, as the name indicates, are generally robust to unmalicious or malicious attacks such as scaling, cropping, lossy compression, and so forth. Robust watermarks may find application in copyright protection for DVD, fingerprinting for recipient tracing and content ownership verification, and so on. In contrast, fragile watermarks are generally designed to be sensitive to any changes in the original digital content. Fragile watermarks are useful for purposes of authentication, i.e., verifying the integrity of a given digital content.

The digital watermarking technology includes two aspects: digital watermarking algorithm designing and digital watermarking algorithm attacking. The research of digital watermarking algorithm attacking is essential for digital watermarking algorithm designing. It is well known that the digital watermark must survive from all kinds of attacks including malicious and unmalicious attacks in the application of copyright protection. However we can always find some potential security problems in previous-presented robust