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

ICIC International ©2010 ISSN 1349-4198
pp. 885–896

IMAGE AUTHENTICATION UNDER DCT DOMAIN WITH ATTACK RECOVERY

Chien-Chang Chen and Husan-An Ke

Department of Information Management
Hsuan Chuang University
Hsinchu 300, Taiwan
cchen34@hcu.edu.tw

Received September 2008; revised February 2009

Abstract. *Image authentication schemes verify the integrity of an image against malicious manipulations. Most image authentication methods treat all manipulations as attacks. However, with the increasing demand for protecting JPEG images, image authentication methods that distinguish JPEG compression from malicious attacks are increasingly needed. This work presents a DCT-based image authentication approach with attack recovery, which recovers the attacked blocks. Two quantization properties, DQP and FQP, are presented to embed authentication features. The embedded feature is tolerant to JPEG compression with a quantization step of less than twice the pre-determined quantization step, but is sensitive to other malicious attacks. The attacked blocks are indicated after verifying a protected image, and the embedded recovery features are then extracted to recover these attacked blocks. Moreover, in case of the damage of recovery feature, an edge-based interpolation recovery approach (EIRA) is proposed to improve recovery results. Experimental results show that the proposed approach efficiently detects and recovers attacked blocks.*

Keywords: JPEG compression, Image authentication, DCT quantization, Image recovery

1. **Introduction.** The Internet pervades daily life owing to its low cost and high efficiency. However, the rapid growth of digital media over the Internet has led to an urgent demand for the copyright and integrity protection, because digital media can be easily replicated and modified. Existing approaches for protection of rights embed robust digital watermarks into multimedia data. In contrast to robust watermarking approaches, fragile watermarks show illegal tampering with images, rather than verifying their ownership. Such schemes are very sensitive to every manipulation when the image is tampered off and can identify the damaged areas accurately. Unlike fragile-watermark schemes, semi-fragile watermarking methods detect malicious attacks while allowing specific manipulations such as JPEG, which includes the proposed method. Important works on this topic are discussed as follows.

Walton [9] embedded check-sums in LSB for detecting image tampering. Fridrich and Goljan [5] proposed a self-embedding method, in which an image is embedded into itself in order to protect the image content. Block-based watermarking methods [10] divide an image into blocks, and insert a robust watermark into each block. To verify the integrity of an image, the authenticator checks the existence of the watermark in all blocks. Chang *et al.* [1] adopted SVD to decompose an image to bases and then embedded information to the least important non-zero coefficients. Chen and Kao [2] embedded reversible watermarks into patterns with two zeros of quantized DCT coefficients. Zhang and Zhao [12] adopted fractal image decoding to descript an image. Lin and Chang [6]