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

ICIC International ©2010 ISSN 1349-4198
pp. 1435–1446

MULTIPURPOSE IMAGE AUTHENTICATION METHOD BASED ON VECTOR QUANTIZATION

Chih-Hung Lin*, Yu-Chiang Li, Hsiao-Fen Chien and Sheng-Lung Chien

Department of Computer Science and Information Engineering
Southern Taiwan University
No.1, Nantai St, Yung-Kang City, Tainan County 710, Taiwan
chuck@mail.stut.edu.tw

Received February 2009; revised May 2009

Abstract. *Many image authentication methods have been proposed over the last decade; however, most methods provided only to focus single purpose. This paper presents a multipurpose image authentication scheme based on vector quantization (VQ), and combined functions with copyright protection, integrity verification, and distinguishes between malicious and non-malicious attack simultaneously. The authentication information is calculated from the VQ index tables of an original image and a lower bound image, and if the image has suffered attack, the correlation coefficient is adopted to find the location of the tampering. The experimental results show that this scheme clearly distinguishes non-malicious manipulation from others, verifies ownership and locates the regions that have been tampered with.*

Keywords: Multipurpose image authentication, Robust, Semi-fragile, Copyright protection, Vector quantization

1. **Introduction.** As a result of the explosive growth of digital multimedia techniques and the broad distribution of digital images over the Internet, people can obtain digital media readily. However, these media may be modified and attacked easily; therefore, digital image copyright protection and content authentication are major issues. Image authentication method can be roughly classified into three categories: robust, fragile and semi-fragile. Robust authentication schemes [5,10,12,17,19] for copyright protection are used for verification of ownership if digital images suffer attack. Fragile authentication schemes [3,4,6,13] for digital content verification are used to detect whether digital images have been altered and to distinguish altered areas from the extracted watermark without using the original images. Semi-fragile authentication schemes [7,11,22,18] are able to accept non-malicious manipulations such as lossy compression while rejecting malicious manipulations. For example, in Lin and Chang [11] scheme, the image feature is generated by the invariant feature before and after lossy compression and embedded into the middle frequency coefficients of discrete cosine transform (DCT) blocks. Lin and Chang scheme can accept JPEG lossy compression and moderate brightness adjustments. Zhou et al. [22] scheme extracts a signature as a watermark from the original image and embeds it into the image using wavelet coefficients. The scheme accepts non-malicious manipulations such as JPEG compression and rejects malicious manipulations such as cropping and replacement processes.

Because of the increase in requests for practical applications in recent years, a multipurpose image authentication scheme has become necessary. Some methods have been