International Journal of Innovative Computing, Information and Control
Volume **7**, Number **7(A)**, July **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **3645–3657**

AUTHENTICATION AND CROSS-RECOVERY OF MULTIPLE IMAGES

Lee Shu-Teng Chen[1], Shang-Kuan Chen[2] and Ja-Chen Lin[3]

[1]Cloud Computing Research Center
Industrial Technology Research Institute
195, Sec. 4, Chung Hsing Rd., Chutung, Hsinchu 310, Taiwan
stlee@itri.org.tw

[2]Department of Computer Science and Information Engineering
Yuanpei University
No.306, Yuanpei Street, Hsinchu 300, Taiwan
cotachen@gmail.com

[3]Department of Computer Science and Information Engineering
National Chiao Tung University
1001 University Road, Hsinchu 300, Taiwan
jclin@cis.nctu.edu.tw

Received February 2010; revised May 2010

Abstract. *This work presents an authentication and cross-recovery scheme to protect a group of n JPEG images. Given n images, the images are scaled down and then encoded using JPEG to create n recovery data. Based on a pre-determined threshold t, $2 \leq t < n$, the n recovery data are shared to create n shadows. Next, n authentication data are generated to identify malicious attacks on the system. Additionally, the n shadows and the n authentication data are embedded in the n JPEG codes of the n original images to form n JPEG stego codes, which can be stored in a distributed storage system. Moreover, in the daily maintenance of the storage system, the authentication data concealed inside these n JPEG stego codes are used to verify which ones have been attacked. If some (up to $n - t$) of the n JPEG stego codes are corrupted, the corrupted JPEG images can be recovered approximately using any t survived JPEG stego codes. Experimental results demonstrate the effectiveness of the proposed method. Comparisons with other image recovery methods are also included.*

Keywords: Cross recovery, Image authentication, Reed-Solomon codes, JPEG

1. **Introduction.**

Retrieval, authentication and recovery of images have received considerable attention in the field of digital images. Sudhamani and Venugopal [1] developed an image retrieval system based on a non-parametric classification technique. Su *et al.* [2] evaluated the performance of a caching algorithm capable of retrieving scalable image contents. Besides the retrieval of images, the relatively easy copying and illegally distribution of digital images through the Internet explain the need to protect the integrity of digital images. Image authentication schemes generally embed authentication data in an image, in which such data can then be extracted to detect changes in the image [3-6]. Chang and Lin [6] obtained nearly optimal positions for embedding authentication data by using a genetic algorithm. Chen *et al.* [7] developed a model to protect digital contents based on group-based authentication and a secret sharing scheme.

Some authentication methods can even recover the tampered portion of an image [8-12]. For instance, Chang *et al.* [10] used vector quantization (VQ) to compress a protected image, and then generated recovery data by sharing the created VQ file. Lin *et al.*