International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **2**, February **2010**

 ISSN 1349-4198
pp. 677–685

SHARING AN IMAGE WITH CHEATER IDENTIFICATION

Chien-Chang Chen and Guang-Yau Suen

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

Received June 2008; revised December 2008

Abstract. *This work presents a novel approach for sharing secret images between participants and identifying cheaters during recovery. The proposed method employs a random image to create a difference image, which represents the difference between the random image and the secret image, and a hash function to calculate verification data, which is the collection of hash results for each shared image. When recovering the secret image, the hash results of each collected shared image are calculated to compare with the verification data as verifying the validity of the shared image. Then, by adding the public difference image and the Lagrange interpolation results of an adequate number of corrected shared images, the secret image can be reconstructed. Size changes in the shared image and public data load are discussed. Property comparisons with other works are also provided.*
Keywords: Secret image sharing, Cheater identification, Hash function

1. **Introduction.** Given the easy modification of digital images, a method of protecting digital images is urgently required. The secret image sharing scheme proposed in this study solves this image security problem by sharing digital images secretly. Traditional secret image sharing approaches generate several shared images from one secret image and calculate the reconstructed image from different shared images.

Secret image sharing approaches can be divided into two categories: *piling up* and *mathematical calculation*. The first approach piles up shared images to obtain a visually similar secret image. Naor and Shamir [8] first introduced the secret image sharing problem and proposed the piling-up approach for sharing a binary secret image. Blundo *et al.* [1] extended the Naor and Shamir technique to sharing a gray-level image. Hou [5] applied the halftone and the color decomposition methods to share a color image secretly. Nakajima and Yamaguchi [7] presented a method of sharing a secret image with two other images and the secret image can be reconstructed by stacking these two images.

The *mathematical-calculation* method mathematically calculates the reconstructed image from shared images. Thien and Lin [11] first adopted a mapping key to permute the secret image and then adopted the Shamir method [10] of secret sharing to generate shared images. Chen and Lin [4] presented a progressive secret image sharing approach in which the number of shared images improves the quality of the reconstructed image. Chen and Chien [3] presented a method of sharing many secret images in which each participant possesses only one shared image. However, none of them discusses the correctness of each shared image in recovering the secret image. This weakness enables malicious attackers synthesizing fake shared image to cheat other correct shared images. This study presents an efficient approach for verifying the correctness of collected shared images when recovering the secret image to prevent others cheating correct shared images.