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

ICIC International ©2010 ISSN 1349-4198
pp. 1165–1178

IMAGE SHARING WITH STEGANOGRAPHY AND CHEATER IDENTIFICATION

Meng-Hsiun Tsai[1], Yang-Bin Lin[2] and Chung-Ming Wang[2]

[1]Department of Management Information Systems
Institute of Bioinformatics
National Chung Hsing University
Taichung, Taiwan
mht@nchu.edu.tw

Department of Computer Science
National Chung Hsing University
Taichung, Taiwan

Received August 2008; revised December 2008

Abstract. *In 2004, Lin and Tsai applied the concept of a threshold secret sharing scheme and the method of parity check to design a secret image sharing and authentication mechanisms. However, cheaters can easily counterfeit a fake stego-image in Lin and Tsai's scheme. In order to overcome this problem, Yang et al. proposed an improved scheme to prevent the users from making a fake stego-image. While Yang et al's scheme embeds just one pixel of secret image into each block, it doesn't meet the property of high-capacity. Furthermore, the modular number in their scheme is 2^8 rather than a prime number. Thus, the secret image cannot be successfully reconstructed from t stego-images in their scheme. In this paper, we will propose an improved scheme which can not only embed t pixels of secret image into each block but also the reconstructed secret image can be established. Moreover, we apply the* Data Signature Algorithm *(DSA) for cheater identification.*

Keywords: Steganography, (t,n) threshold secret sharing

1. **Introduction.** Nowadays, due to the rapid development of the Internet, it is very common and popular to deliver data such as audio and images as well as text via the network. How to protect these data becomes extremely significant, especially secret data.

The most common schemes for protecting secret data are encryption [2, 6, 7, 10, 13]. Encryption means that encrypts the secret data to form a ciphertext with a secret key, and the secret data can be recovered with the same secret key. Ciphertext is meaningless data which will result in attracting others' attention and further reveal the existence of secret data. Unlike the encryption, steganography [3, 4, 5, 11, 14, 15, 17, 21, 22, 23, 25, 27, 28], is to embed the secret data into a cover-media such as images, audios, as well as videos, and then obtains a stego-media. Stego-media is meaningful, thus it is not easy to perceive the existence of secret data. Therefore, it is needless to say that steganography provides a better security than encryption. The most common and simple steganographic scheme directly replaces *Least Significant Bits* (LSBs) of the pixel in a cover-image with the secret bits.

Generally speaking, a good steganography scheme must meet the following requirements [12].

1: Better image quality [4, 21]: The stego-image containing secret data must keep the property of imperceptibility. In other words, other people except legal users cannot detect the existence of secret data from the stego-image.