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

ICIC International ©2011 ISSN 1349-4198
pp. **3923–3937**

A CHEAT-PREVENTING VISUAL CRYPTOGRAPHY SCHEME BY REFERRING THE SPECIAL POSITION

Chwei-Shyong Tsai[1], Hao-Cheng Wang[2], Hsien-Chu Wu[3] and Chung-Ming Wang[2,*]

[1]Department of Management Information Systems
[2]Institute of Computer Science and Engineering
National Chung Hsing University
No. 250, Kuo Kuang Road, Taichung 402, Taiwan
tsaics@nchu.edu.tw; wanghc.tw@gmail.com
*Corresponding author: cmwang@cs.nchu.edu.tw

[3]Department of Computer Science and Information Engineering
National Taichung Institute of Technology
No. 129, Sec. 3, Sanming Road, Taichung 404, Taiwan
wuhc@ntit.edu.tw

Received January 2010; revised June 2010

Abstract. *Visual cryptography (VC) is an effective and a secure scheme for sharing a secret image with the participants. VC scheme encodes the secret image into the shares. Each participant holds one share. When the participants stack a sufficient number of shares, the secret image can be decrypted through the human visual system. However, in some situations, cheating is possible in the VC scheme. The dishonest participant, called a cheater, may provide a fake secret image to cheat the other participants. In this paper, we proposed a cheating scheme to prove that the cheater can cheat other participants in Hu and Tzeng's cheat-prevention scheme [1]. To achieve cheat-prevention in VC, we propose a novel transformation scheme. The proposed scheme can recognize the fake share by stacking shares in a special position in the verification stage. In our scheme, we can improve Hu and Tzeng's cheat-preventing scheme and transform the existing VC scheme into the cheat-prevention scheme. Moreover, our scheme does not need an extra verification share which would reduce the burden of share management for each participant.*

Keywords: Visual cryptography, Visual secret sharing, Cheat-preventing

1. **Introduction.** The secret image sharing scheme is a technique for sharing a secret image with the participants. The secret image can be reconstructed through a particular computing manner, when the participants provide sufficient information. However, in the decrypting stage, it usually requires several decoding computations to reconstruct the secret image. Naor and Shamir proposed a novel secret sharing scheme to share the secret image, called visual cryptography (VC) [2]. The main feature of the VC scheme is to use the human visual system to decode the secret information without decoding computation. VC scheme encrypts the secret image into a set of shares. Each share is usually printed on transparent and then given to a different participant. When the participants stack the sufficient shares, the secret information can be viewed on the stacked shares. Furthermore, a (k, n)-VC scheme encrypts the secret image into n shares. By stacking any k or more shares together, the secret information can be reconstructed. If the stacked shares are less than k, there is no information about the secret image.