International Journal of Innovative Computing, Information and Control
Volume **7**, Number **11**, November **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 6411–6421

HIGH CAPACITY DATA HIDING IN REVERSIBLE SECRET SHARING

Zhenfei Zhao[1], Ka-Yin Chau[2] and Zhe-Ming Lu[1,3,*]

[1]School of Information Science and Technology
Sun Yat-sen University
No. 135, Xingangxi Road, Haizhu District, Guangzhou 510275, P. R. China
tree1118220@126.com

[2]Hong Kong Quality Management Association
PO Box 2867, General Post Office, Hong Kong

[3]School of Aeronautics and Astronautics
Zhejiang University
No. 38, Zheda Road, Hangzhou 310027, P. R. China
[*]Corresponding author: zheminglu@zju.edu.cn

Received June 2010; revised October 2010

Abstract. *Recently, a reversible secret sharing scheme has been developed for encrypting a secret image in a set of camouflage images. The key advantage lies in that both the secret and cover images can be accurately reconstructed during decryption. This paper proposes a high capacity data hiding scheme integrated in reversible secret sharing. In secret sharing, some extra confidential data are also hidden in camouflage images by means of a double module mechanism. As a multilevel histogram shifting strategy is employed, a high capacity can be achieved. In the decoder, not only the cover and secret images but also the confidential data can be perfectly recovered. The confidential data can be some affiliated information of the secret image or for validity authentication. Experimental results demonstrate the effectiveness of the proposed method.*

Keywords: Reversible secret sharing, Data hiding, High capacity

1. Introduction.

Secret sharing plays an important role in data encryption. In [1], Shamir et al. proposed a (r, n)-threshold prototype based on Lagrange polynomial interpolation. In this model, the secret data are encrypted into n shares. If r or more than r shares are polled, the secret can be decrypted. Otherwise, if $r - 1$ or fewer shares are collected, no meaningful information can be revealed. In [2], Thien et al. extended Shamir's model into image secret sharing, i.e., hiding a secret image in a set of noise-like shadow images. Visual cryptography [3] is another useful technique for image secret sharing. It employs the properties of human visual system and thus maintains the advantage that the secret content can be viewed via stacking a qualified set of shadow images. This stack-to-see mechanism makes it applicable in the applications where no computer is aided.

Besides secret sharing, data hiding [4,9,10] is also widely used in multimedia security. There are many data hiding methodologies in the form of diverse algorithms. Many activities aiming at improving the overall hiding performance are currently ongoing. In recent years, researchers have paid much attention to lossless data hiding; i.e., both the confidential data and the host image can be accurately recovered in the decoder. Therefore, it is useful in the applications where the host images (e.g., military maps, remote sensing images, medical images, digitalized art pictures) are required to be exactly reconstructed.