International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **12**, December **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 5749–5769

A VISUAL SHARING SCHEME FOR MULTIPLE SECRETS BY CAMOUFLAGING PROCESS

Tsung-Lieh Lin[1], Shi-Jinn Horng[1,2,*], Kai-Hui Lee[3], Pei-Ling Chiu[4]
Tzong-Wann Kao[5], Ray-Shine Run[6], Jui-Lin Lai[6] and Rong-Jian Chen[6]

[1]Department of Electrical Engineering
[2]Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology
Taipei, Taiwan
jabezlin@yahoo.com.tw
*Corresponding author: horngsj@yahoo.com.tw

[3]Department of Computer Science and Information Engineering
[4]Department of Risk Management and Insurance
Ming Chuan University
Taipei, Taiwan
{ khlee; plchiu }@mail.mcu.edu.tw

[5]Department of Electronic Engineering
Technology and Science Institute of Northern Taiwan
Taipei, Taiwan
tkao@ms6.hinet.net

[6]Department of Electronic Engineering
National United University
Miao-Li, Taiwan
run5116@ms16.hinet.net; { jllai; rjchen }@nuu.edu.tw

Received August 2009; revised February 2010

Abstract. *Many studies have been published related to the model of visual cryptography proposed by Naor and Shamir. Most of these studies concentrate on how to share a single secret on the generated shares; although few of them focus on the sharing of multiple secrets, there are still pixel expansion and low contrast problems. By reviewing the related literatures on visual secret sharing schemes for multiple secrets (VSSM schemes), the pixel expansion is at least 2x for sharing m secrets, and the contrast is at most 1/2x. In this paper, we propose a novel VSSM scheme that is different from all previous schemes. Our approach, which is based on the secret separating and camouflaging processes, not only can generate non-expansion shares but also obtain higher contrast on recovered images without the need to redesign the codebook. Experimental results show that the proposed scheme has achieved better performance than all of the existing VSSM schemes.*

Keywords: Visual cryptography, Multiple-secret-sharing scheme, Camouflaging process, Pixel expansion

1. **Introduction.** Naor and Shamir proposed a secure cryptographic method, called the Visual Cryptography (VC), to hide secrets of image form [1]. The encrypted secret images of VC could be revealed by directly stacking two share images that can be recognized by human visual, without any computation or the use of any devices. For some environments without available devices to decrypt the share images, the VC scheme was a perfect and convenient way to share secrets. Moreover, visual cryptography has been applied in many