

MEANINGFUL SHADOW BASED MULTIPLE GRAY LEVEL VISUAL CRYPTOGRAPHY WITHOUT SIZE EXPANSION

PEI-YAN PAI¹, CHIN-CHEN CHANG^{1,2,4}, YUNG-KUAN CHAN^{3,*}
AND CHI-CHENG LIAO⁴

¹Department of Computer Science
National Tsing Hua University
No. 101, Sec. 2, Kuang-Fu Road, Hsinchu 300, Taiwan
d938338@oz.nthu.edu.tw

²Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wenhwa Road, Seatwen, Taichung 407, Taiwan
ccc@cs.ccu.edu.tw

³Department of Management Information Systems
National Chung Hsing University
No. 250, Kuokuang Road, Taichung 402, Taiwan
*Corresponding author: ykchan@nchu.edu.tw

⁴Department of Computer Science
National Chung Cheng University
No. 168, University Road, Minhsiung Township, Chiayi County 621, Taiwan
lcc96m@cs.ccu.edu.tw

Received October 2009; revised February 2010

ABSTRACT. *In traditional visual cryptographic methods, a reconstructed secret image is usually at a binary gray level and is expanded in size, and the created shadow images often appear meaningless and noise-like. This paper will provide a meaningful shadow based multiple gray level visual cryptography without size expansion (MSML) method. This method not only creates a reconstructed secret image with multiple-gray levels and without size expansion, but the created shadow images also appear similar to the cover images specified by the user. Moreover, a user can adjust the qualities of the reconstructed secret image and the shadow images according to his requirements.*

Keywords: Image hiding, Visual cryptography, Visual secret sharing

1. Introduction. Along with the rapid development of the Internet technology, security is an important issue for the protection, authentication and privacy of confidential data delivered via networks [5]. In recent years, many data embedding methods, such as image hiding [4,9], secret sharing [6,10,12,13], have been proposed to avoid seizure of confidential data. However, these methods require complex computations for decoding. Naor and Shamir [7] proposed a visual cryptography (VC) method that can reconstruct, without any computations, the secret image by collecting the shadow images for identification via the human visual system.

The VC method can be extended to a (k, n) visual secret sharing (VSS) method [7]. In a (k, n) VSS method, a secret image is encoded into n noise-like shadow images or transparencies. When any k or more shadow images are assembled together, the secret image is revealed. However, stacking fewer than k shadow images cannot reveal any information about the secret image.