International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **5**, May **2010**

 ISSN 1349-4198
pp. **2089–2102**

REVERSIBLE DATA HIDING IN TWO STEGANOGRAPHIC IMAGES USING MATRIX CODING

Chi-Shiang Chan[1] and Ching-Yun Chan[2]

[1]Department of Information Science and Applications
Asia University
Wufeng 41354, Taiwan
CSChan@asia.edu.tw

[2]Computing Laboratory
Oxford University
Oxford, United Kingdom
Ching.Yun.Chang@comlab.ox.ac.uk

Received October 2008; revised April 2009

Abstract. *In this paper, we propose a reversible data hiding method of high embedding efficiency. By referring to secret data, the method first applies Matrix Coding to determine the modified position of a seven-bit unit in the cover image. The method presented here requires only one bit, the position bit, to record the modified position for each seven-bit unit. The position bits will be appended to secret data and treat as a part of secret data. Then, the appended secret data are embedded in cover images by applying Matrix Coding. In the extracting phase, the secret data and the position bits are extracted from the hidden data. The position bits are used to reconstruct the original cover image, which can be recovered without any loss. The experimental results show that PSNR values of stego images are higher than 57 and thus our proposed method can produce high quality steganographic images.*

Keywords: Image hiding, LSB matching revisited, Reversible data hiding

1. **Introduction.** Digital Steganography is a technique that embeds secret data in meaningful multimedia data, such as video and images, by making small changes to cover media that are below the level of human perception. There are two important criteria for Digital Steganography. One is the security of the secret data and the other is the camouflage ability of stego images. When we take the security of secret data into consideration, data encryption methods, such as DES and RSA, are used to encrypt secret data before the embedding process. As for the camouflage ability of stego images, the quality of cover images should not be degraded too much after the embedding process, otherwise grabbers can be aware of the changes. Generally speaking, a good quality stego image is unsuspicious and damage-avoidable to grabbers. Therefore, data hiding techniques do not need to consider attacks on stego images. Instead, they pay more attention to the camouflage ability.

There are different kinds of data hiding methods for different kinds of cover images. For example, [7,8,15] hide secret data in halftone images, [14,17] use image compression methods to achieve data hiding, and [6] applies SVD technique to hide data. However, the quantity of embedded data in these methods is quite limited. Another data hiding approach is the least-significant-bit (LSB) substitution technique [1-3], in which the least significant bits of the cover pixels are replaced with secret data. Although LSB replacement is a straightforward way and has satisfied data carrying capacity, it causes a phenomenon called asymmetric modification that either increases even-valued pixels