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

 ISSN 1349-4198
pp. 5797–5807

A DIGITAL IMAGE AND SECRET MESSAGES SHARING SCHEME USING TWO STEGO IMAGES

Chang-Chu Chen[1,2] and Chin-Chen Chang[1,3]

[1]Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi 62102, Taiwan
{ ccz; ccc }@cs.ccu.edu.tw

[2]Department of Management Information System
Central Taiwan University of Science and Technology
Taichung 40601, Taiwan
ccchen@ctust.edu.tw

[3]Department of Information Engineering and Computer Science
Feng Chia University
Taichung 40724, Taiwan

Received August 2009; revised December 2009

Abstract. *This paper proposes a novel reversible data-hiding algorithm that can losslessly recover the original image from two embedded images after the hidden data have been extracted. In general, data-hiding schemes embed secret data into the cover medium and generate a single embedded medium. Once the single embedded medium has been captured, the hidden secret data may no longer be secure. Therefore, we use the proposed method to embed secret data into multi-embedded media to address this drawback. The experimental results show that our method outperforms other reversible data-hiding methods in terms of payload versus distortion.*
Keywords: Data hiding, Reversible, Secret sharing, Payload

1. **Introduction.** The goal of data hiding [16] is to conceal secret messages in harmless media without obvious distortion in order to prevent malicious tampering. The data hiding process integrates original media data and embedding data into embedded media data. Data hiding can be used in many practical applications [17]. For instance, in covert communications, steganography [19] aims to imperceptibly hide secret data in a commonly cover medium, so that the presence of the embedded data cannot be easily detected. For the protection of intellectual property rights [13], digital media owners can embed copyright data using digital watermarking [4,11,14]. There are two essential requirements for a data hiding scheme to be successful [8]. First, the degradation of the original media should be minimized. Second, hiding capacity or called payload size, which is the amount of data that can be hidden and extracted from embedded media, should be maximized. However, embedding distortion and capacity are mutually exclusive.

In most cases of data hiding, the embedded media will be distorted to a certain degree and cannot be fully restored after the hidden data have been extracted. For some applications or sensitive images, such as medical diagnosis, law enforcement, military images and medical images, even the slightest alteration in pixel values is unacceptable. Thus, it is critical to restore the media. To ensure that a sensitive image can be completely recovered after the hidden data are fully extracted, reversible, lossless, distortion-free or invertible data hiding techniques are used [6,10,15].