International Journal of Innovative Computing, Information and Control
Volume **5**, Number **11(B)**, November **2009**
ICIC International ©2009 ISSN 1349-4198
pp. 4283–4289

LSB-BASED HIGH-CAPACITY DATA EMBEDDING SCHEME FOR DIGITAL IMAGES

Chia-Chen Lin[1], Yi-Hui Chen[2] and Chin-Chen Chang[3]

[1]Department of Computer Science and Information Management
Providence University
Taichung 43301, Taiwan
mhlin3@pu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chung Cheng University
Chiayi 621, Taiwan
chenyh@cs.ccu.edu.tw

[3]Department of Information Engineering and Computer Science
Feng Chia University
Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

Received July 2008; revised December 2008

Abstract. *In this paper, an improved LSB replacement scheme having a high payload is proposed. In this scheme, a secret stream is transformed into a secret sequence by using a 3^n-base notational system and the secret sequence is embedded into a pixel unit containing n neighboring pixels. On average, $log_2 3$ bits can be embedded into a cover pixel; therefore, our proposed data embedding scheme outperforms the original LSB replacement technique in hiding capacity. Experimental results present positive data that confirm that our proposed scheme not only provides higher hiding capacity than LSB replacement at the same image distortion levels, but also resists LSB attack and detection.*

Keywords: Data embedding, Hiding capacity, Stego-images, LSB replacement, LSB attack

1. **Introduction.** Steganography is one branch of data embedding [1, 2, 3, 4, 8, 9, 10, 11, 12] which is a technique widely used to conceal secret data in cover media, such as images, videos, electronic documents, or any other digitized medium. In the past, several steganography schemes [1, 2, 3, 4, 8, 9, 10, 11, 12] have been proposed to embed the secret data into the cover media. Because embedded media generated by steganographic schemes is perceptually undetectable and nonstatistical, hidden secret data can be securely transferred to the receiver side without raising any suspicion on the part of potential attackers. There are two criteria used to evaluate the performances of steganography schemes, namely embedding capacity and visual quality of stego-image. Generally, high performances of steganography schemes imply high embedding capacity and good image quality of stego-images; although embedding capacity and image quality are tradeoff.

Among all the steganography schemes, LSB-based (least significant bit plane) embedding strategies [9, 10, 12] were widely used for its high hiding capacity, and simpleness to realize. Up to now, LSB-based strategies can be categorized into two basic types: LSB replacement and LSB matching. The former replaces the least significant bits of pixels with secret data in a cover image. The latter first converts the secret data into a stream of bits. Later, the LSB of the cover pixel value is added or subtracted if the LSB of the next cover pixel does not match the next bit of secret data; otherwise, the LSB of the