International Journal of Innovative Computing, Information and Control
Volume **7**, Number **11**, November **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 6203–6218

A REVERSIBLE WATERMARKING SCHEME WITH HIGH PAYLOAD AND GOOD VISUAL QUALITY FOR WATERMARKED IMAGES

The Duc Kieu[1] and Chin-Chen Chang[2]

[1]Department of Computing and Information Technology
The University of the West Indies
St. Augustine, Trinidad and Tobago
ktduc0323@yahoo.com.au

[2]Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wen-Hwa Road, Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

Received June 2010; revised October 2010

Abstract. *High embedding capacity, good visual quality and reversibility are desired factors of information hiding systems. Recently, Thodi and Rodriguez proposed a reversible watermarking method with high embedding capacity. However, embedding capacity and image quality of this method can be improved. Thus, we propose a reversible watermarking scheme inspired by the prediction error expansion (PEE) embedding technique proposed by Thodi and Rodriguez. The proposed method embeds three secret bits into one grayscale cover pixel at a time by using a pixel partition strategy. Experimental results show that the proposed method achieves high embedding capacity measured by bit per pixel (bpp) and good visual quality measured by peak signal-to-noise ratio (PSNR). Specifically, the embedding capacity of the proposed method is about 1.4 times higher than that of the PEE method for all test images. The PSNR value of the proposed method in the range of embedding capacity [0.1, 1) is at least 13 dB higher than that of the PEE method for all test images. The PSNR value of the proposed method at its maximum embedding capacity (around 1.4 bpp) is always greater than 39 dB for all test images. In addition, the proposed method surpasses many existing reversible watermarking methods.*

Keywords: Reversible watermarking, Prediction error expansion (PEE), Expansion embedding, Data embedding, Information hiding

1. Introduction.

Advances in network technology facilitate digital multimedia delivery. However, sending digital multimedia (e.g., digital images, videos, audios and texts) over public networks such as the Internet is insecure because of counterfeiting, forgery, fraud and copy violation. Therefore, methods for protecting digital data, especially confidential data, are highly needed. Traditionally, secret data can be protected by cryptography. In cryptographic methods, secret messages can be encrypted prior to distribution by using data encryption standard (DES) [21] or RSA [22]. However, the weakness of cryptography is that it can protect secret messages in transit, but once they have been decrypted, the content of secret messages has no further protection [12]. Thus, an alternative method used to protect secret data is information hiding.

Information hiding includes steganography and digital watermarking [10]. Steganography is used for secure communications among parties. Steganographic systems undetectably modify a cover object (i.e., a message carrier) to embed a secret message by using information hiding (also called data hiding or data embedding) techniques [12]. Thus, steganography is used to protect the existed secret message from being discovered