International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **3**, March **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 1375–1385

REVERSIBLE DATA HIDING FOR VQ INDICES USING PREDICTION ERRORS

Zhi-hui Wang[1], Chin-Chen Chang[2,*], Huynh Ngoc Tu[2] and Ming-Chu Li[1]

[1]School of Software
Dalian University of Technology
Dalian, P. R. China
wangzhihui1017@yahoo.cn; li_mingchu@yahoo.com

[2]Department of Information Engineering and Computer Science
Feng Chia University
No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
ngoctu84vn@gmail.com
*Corresponding author: ccc@cs.ccu.edu.tw

Received October 2009; revised February 2010

Abstract. *Reversible data hiding techniques have received more and more attention in recent years. Many researchers have proposed methods to directly hide secret data in an image. However, images are usually compressed and stored using compression techniques in indices format. Hence, this paper proposes a novel and reversible data hiding method for vector quantization (VQ) compressed images. The proposed scheme exploits characteristics of VQ indices and the prediction errors between them to embed the secret data and to guarantee that the original indices can be recovered to reconstruct the VQ compressed image. The experimental results show that the proposed method can achieve higher embedding capacity and better bit rate compared to other schemes.*
Keywords: Steganography, Vector quantization, Principle component analysis

1. **Introduction.** With the rapid development of communications over the Internet, a huge amount of digital data is transmitted over the Internet every day. As we know, the Internet is an open channel for transmitting information. Then, how to protect the privacy and security of these transmitting data becomes a more crucial task. For example, if a British doctor wants to send a patient's x-rays and medical records to a doctor in America via the Internet, the medical records of the patient should be protected as a secret message for reasons of privacy. Several encryption approaches just encrypt secret messages into an unrecognizable form. However, meaningless encrypted messages can attract the attention of attackers during transmission. To remedy this problem, the information hiding schemes that embed secret data into cover objects such as written texts, digital images, and videos have been proposed by many researchers. As to the above-mentioned example, the British doctor can use the information hiding scheme to embed the patient's medical records into his x-rays and then send the x-rays to the doctor in America via the Internet without arousing suspicion.

In general, information hiding schemes can be divided into two categories depending on the relationship between the embedded message and the cover image. In the first category, digital watermarking [1,2] and the embedded message that are used to authenticate the cover image has a close relationship with the cover image. In the second category, Steganography [3,4], in which the embedded message has no relationship with the cover object, aims to mask the existence of the secret information. Steganography techniques can be performed in three domains, i.e., the spatial domain [5], the frequency domain,