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

 ISSN 1349-4198
pp. 2701–2713

DATA HIDING FOR INDEX-BASED IMAGES USING OVERLAPPING CODEWORD CLUSTERING AND RUN LENGTH CONCEPT

Piyu Tsai

Department of Computer Science and Information Engineering
National United University
Miaoli 36003, Taiwan
pytsai@nuu.edu.tw

Received January 2009; revised May 2009

Abstract. *Hiding data on index-based images always suffers from low hiding capacity and high image degradation. In this paper, an improved codeword clustering and the run length concept are explored to deal with this problem. The proposed codeword clustering improves Chiang and Tsai's scheme to which a codeword can reside in any size of sub-codebooks. Accordingly, the number of sub-codebooks is increased and a strong similarity among codewords is still preserved. In addition, the structure of secret message is explored by the run length concept to further enhance the hiding capacity.*

Experimental results show that the number of sub-codebooks is increased significantly by the contribution of codeword overlapping to which the number of overlapping codewords is greater than the number of individual codewords. The ratio between the hiding capacity and the embedding distortion shows the proposed embedding efficiency. In comparison with some similar schemes, the average performance of the proposed method works well.
Keywords: Overlapping codeword clustering, Data hiding, Index-based image

1. **Introduction.** Data hiding is a technique used to conceal a secret message inside ordinary material [2]. The secret message is imperceptibly embedded into the cover material. The cover material with the secret message is called stego-material. The difference between cover material and stego-material is generally difficult to distinguish by the human eyes. Accordingly, the stego-material can be secured on open channels without suspicion. The concept of data hiding is similar to that of camouflage used by many insects to safeguard themselves from being attacked.

Nowadays, digital data hiding techniques have been developed. They conceal a digital secret message into various digital cover materials, such as text, image, audio, video, web page and so on. Digital data hiding has been applied to digital watermarking, multimedia authentication, finger printing, etc. in which the secret message (logo, authentication code, serial number) is embedded and extracted to protect, authenticate or trace the original material [16].

Several data hiding techniques have been proposed. They can be divided into three categories according to the format of the cover material. In the first category, the secret message is directly embedded in the spatial domain of the cover material. The least-significant-bit (LSB) based substitution is the simple and well-known method. Lee and Chen [11] modify the LSBs of a cover image to hide a secret message. Wang et al. employ the optimal LSB substitution and genetic algorithm to embed the secret message [18]. Luo et al. embed a secret message in the LSB plane of the carrier image randomly via a chaotic system, then makes a dynamic compensation on the stego-image to against some steganalysis methods [14]. Wang and Chen propose a two-way block matching method to achieve high-payload and good visual quality [19].