International Journal of Innovative Computing, Information and Control
Volume **3**, Number **3**, June **2007**

ICIC International ©2007 ISSN 1349-4198
pp. **631–640**

A GA-BASED NEARLY OPTIMAL IMAGE AUTHENTICATION APPROACH

Chien-Chang Chen and Cheng-Shian Lin

Department of Computer Science
Hsuan Chuang University
Hsinchu 300, Taiwan
cchen34@hcu.edu.tw

Received February 2006; revised October 2006

Abstract. *In this paper, we present how to find nearly optimal positions for embedding authentication message by Genetic Algorithm (GA), so as to achieve high quality protected image in image authentication problem. Correlations between important DCT coefficients and user defined thresholds constitute the image authentication message. The embedding positions are simulated as chromosomes and we use GA operators, such as reproduction, crossover, and mutation to find nearly optimal embedding positions. Experimental results demonstrate that GA can improve the image quality of protected image effectively.*
Keywords: Genetic algorithm (GA), Image authentication

1. **Introduction.** Recently, massive amounts of data are easily downloaded through the Internet since the rising and flourishing of computer and Internet technology. The convenience of file transmission over networks lets attackers acquire and modify digital content handily. Therefore, the copyright protection has become a very important issue, and this problem can be solved by digital watermark and image authentication techniques.

However, digital watermark differs from image authentication. Digital watermark identifies the legal ownership when a digital watermarked image suffers malicious attacks, but digital watermark cannot detect modification places [3,4,8,11]. Unlike digital watermark, image authentication points out the maliciously altered areas.

The image authentication problem can be classified into watermark-based approach and signature-based approach according to where the signature is located. Both of them extract important features from an image. The watermark-based approach embeds the authentication message into the host image. Thus the embedding quantity must be limited to prevent destroying image quality [1,15]. On the contrary, the signature-based approach stores the authentication message into an extra file and the storage quantity can be much larger than the watermark-based approach [5,14]. However, requiring extra space is a load in signature-based approach.

Besides, in order to reduce image data size, some desirable image compression, such as JPEG, would always be used. Some important works have been proposed to overcome this image compression problem. Extending of Yueng and Mintzer's [17] technique, Wu and Liu [16] proposed schema verification in quantized DCT coefficients via look-up-table. Sun *et al.* [13] discovered that the largest singular value of SVD survives under JPEG