International Journal of Innovative Computing, Information and Control
Volume **6**, Number **7**, July **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 3193–3203

STEGANALYSIS METHOD DEFEATING THE MODIFIED PIXEL-VALUE DIFFERENCING STEGANOGRAPHY

Cong-Nguyen Bui[1], Hae-Yeoun Lee[2], Jeong-Chun Joo[1]
and Heung-Kyu Lee[1]

[1]Department of Computer Science
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea
hklee@mmc.kaist.ac.kr

[2]School of Computer and Software Engineering
Kumoh National Institute of Technology
Gumi, Gyeongbuk, Republic of Korea

Received January 2009; revised July 2009

Abstract. *Pixel-value differencing (PVD) steganography generates step effects or abnormal high fluctuations in PVD histogram. Since steganalysis exploits these artifacts to defeat the PVD steganography, modified PVD (MPVD) steganography preserving the PVD histogram is recently presented. This paper proposes a novel steganalysis method, in which we embed message one more time into the suspicious image to generate multiple features in image histogram and pixel value differencing histogram. These features are used to defeat the MPVD steganography. In our experiment, the proposed method is tested on more than 2,000 images. The result shows that our method can defeat the MPVD steganography method at high embedding rate.*

Keywords: Steganography, Steganalysis, PVD, RS analysis, PVD histogram analysis

1. Introduction.

Steganography is the science of hiding information whose goal is to hide even the existence of secret messages by embedding the secret messages into an innocent-like cover. On the contrary, steganalysis is the science of detecting the existence of hidden messages in embedded image by steganography (stego-image). Steganalysis researchers try to improve steganalysis methods to defeat steganography methods by exposing their flaws.

Least Significant Bit (LSB) replacement, a popular steganographic scheme, is simple to implement but can be easily detected by targeted steganalysis techniques such as RS [1] and SPA [2], and universal steganalysis such as HCF-COM [3] and steganalysis scheme in [4]. There have been many ways to improve the security of LSB replacement. For example, the steganography scheme in [5] is an enhancement LSB embedding method, which is secure against SPA steganalysis. However, these steganography schemes have very low embedding capacity. The goal of high embedding capacity and security in steganographic schemes can be archived by modifying more than only LSB of the pixel value. Pixel-value differencing (PVD) steganography [6], one of the most well-known steganographic schemes in the spatial domain, can satisfy this goal. PVD steganography [6] not only has higher embedding capacity but also is non-detectable by RS, SPA and HCF-COM. Over LSB replacement schemes, PVD steganography has been improved to increase the security and capacity. For instance, some methods have been proposed such as modified PVD [7], enhanced PVD [8], and modulus PVD [9]. On the steganalysis side, targeted steganalysis method for these PVD steganography methods has been studied. Zhang and Wang [7]