International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **1**, January **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 161–175

ADAPTIVE STEGANOGRAPHIC METHOD USING THE FLOOR FUNCTION WITH PRACTICAL MESSAGE FORMATS

Jeong-Chun Joo[1], Tae-Woo Oh[1], Hae-Yeoun Lee[2] and Heung-Kyu Lee[1]

[1]Department of Computer Science
Korea Advanced Institute of Science and Technology
291 Daehak-Ro, Yuseong-gu, Daejeon, Republic of Korea
hklee@mmc.kaist.ac.kr

[2]School of Computer and Software Engineering
Kumoh National Institute of Technology
77 Sanho-ro (Yangho-dong), Gumi, Gyeongbuk, Republic of Korea

Received June 2009; revised December 2009

Abstract. *This paper proposes a secure steganography to preserve the PVD histogram even though the histogram of the messages is not uniform. Most researchers of steganographic algorithms have assumed that the histogram of the secret data becomes uniform due to encryption. However, although the practical message files for real communication are encrypted, these files do not create a uniform distribution differently from the initial assumption, which has many artifacts in the PVD histogram that could reveal the existence of the hidden message: steps, fluctuations and asymmetric properties. We present an adaptive and secure steganographic method that is tolerant of the distribution of the message and achieves high capacity and good image quality. A floor function is employed for the flexible modification of the PVD histogram. Also, a modulus function is adopted to provide high embedding capacity and good image quality. A TakeFill algorithm adjusts the PVD histogram to look similar to the cover image. Experimental results support that the proposed method achieves the security while providing maximum hiding capacity and good image quality.*

Keywords: Steganography, Steganalysis, Pixel-value differencing, Histogram adjusting, Practical messages

1. **Introduction.** Steganography is the art and science of concealing the very existence of the secret data. Capacity and imperceptibility are two important factors that lead to successful steganography. These factors naturally contradict each other because embedding large payloads of the secret data into the cover causes many artifacts, which increases the chances that the existence of the hidden message will be detected. Many researchers have studied whether modern steganography is secure in relation to high capacity and good imperceptibility and whether it still preserves the statistical properties [1, 2]. In particular, some researchers specifically studied image communication [3, 4, 5]. For sensitive data such as medical and military images, since they do not allow any losses, a reversible data hiding schemes are studied [6, 7, 8].

Great differences between the cover and stego-image make the steganography insecure. The human eye can distinguish the stego-image from the cover image by looking at the distortions in the stego-image. Moreover, steganalysts can try to use the statistical artifacts generated from the embedding process to detect the existence of the hidden message [9, 10].

Pixel-Value Differencing (PVD) steganography embeds more bits of secret data into pixel pairs that have large differential values such as the edge. After Wu and Tsai proposed