Anti-Forensics for Unsharp Masking Sharpening in Digital Images

Lu Laijie, School of Information Science and Engineering, Hunan University, Changsha, China

Yang Gaobo, School of Information Science and Engineering, Hunan University, Changsha, China

Xia Ming, School of Information Science and Engineering, Hunan University, Changsha, China, & College of Electrical & Information Engineering, Southwest University for Nationalities, Chengdu, China

ABSTRACT

As a retouching tool, image sharpening can be applied as the final step to hide those possible forgery operations in an image. Unsharp masking (USM) is a popular sharpening method supported by most image editing software such as Adobe Photoshop. Several passive forensics methods have been presented for the detection of USM Sharpening. In this paper, an anti-forensic scheme for USM Sharpening is proposed to invalidate the existing forensic algorithms. It removes the overshoot artifacts in image edges and abrupt change in histogram ends. The effectiveness of the proposed method is proved by the experimental results on a large image database with various parameter settings. Comparisons are made among the unsharpened images, the sharpened images and the anti-forensic dithered image. Both the detection ability and image quality are used for its performance evaluation.

Keywords: *Anti-Forensics, Anti-Forensic Dither, Image Forensics, Overshoot Artifacts, Sharpening Detection*

INTRODUCTION

The widespread availability of Internet, together with the rapid popularity of digital cameras has resulted in rich digital images in our daily life. However, digital images can be easily manipulated by various editing software such as Adobe Photoshop. This has created an environment where the authenticity of digital images is often in doubt. To prevent the use of forged/tampered images in news report and court evidence, digital image forensic has attracted great research interests. Especially, since passive image forensics does not need any auxiliary

DOI: 10.4018/jdcf.2013070104

data such as watermark or signatures, a variety of passive image forensic schemes have been developed (Li & Li, 2012). The most representative works about passive image forensic can be divided into two categories. The first class of forensics methods concentrate on identifying those content-changing image manipulations, including image splicing (Weir & Lau, 2010), and copy-move (Ferrara & Bianchi, 2012; Peng & Nie, 2011), which change the image content both visually and semantically. These content-changing manipulations are usually malicious forgery operations worthy of serious attention from the public, since they will influence people's understanding towards the content of digital image. For image copy-move, it can be localized via fine-grained analysis of color filter array (CFA) artifacts or compound statistical features. And an evaluation of popular copy-move forgery detection approaches is summarized in (Christlein & Riess, 2012). The second class of forensics methods focus on those image manipulations which do not change the image content, such as resampling (Mahadian & Saic, 2008), JPEG compression (Fan & Queiroz, 2003), contrast enhancement (Stamm & Liu, 2008; Stamm & Liu, 2010), median filtering (Cao & Zhao, 2010; Kirchner & Fridrich, 2010) and image sharpening (Cao & Zhao, 2009; Cao & Zhao, 2011). However, those content-preserving image manipulations are more easily to be performed since it does not need sophisticated skills by professional users. They are often utilized as post-processing after image tampering to conceal its visual trails. For example, image sharpening is commonly applied as a retouching tool.

Unsharp masking (USM) sharpening is a widely used image sharpening method. The most popular image editing software Adobe Photoshop supports this function for local contrast enhancement. The principle behind USM is exaggerating the light-dark contrast between the two sides of an edge. Therefore, USM might be utilized to hide the tampering trails such as blurriness. In recent years, two blind forensics schemes have been proposed to detect the possible image sharpening. The clues for blind forensics are histogram aberration / ringing artifacts (Cao & Zhao, 2009), and the overshoot artifacts (Cao & Zhao, 2011) occurred around side-planar edges in sharpened images, respectively. Desirable results are obtained for the detection of USM sharpening. It is reported that even for small size images undergone USM sharpening operation, overshoot artifacts could be considered as a dominating feature for the forensics of the USM sharpening operations.

Meanwhile, the research on anti-forensic techniques has been becoming a hot topic in the field of information security. From the information confrontation point of view, anti-forensics is an effective counter-measure to passive forensics since those forgery artifacts left by image tampering are removed or hidden by anti-forensics. In fact, it is particularly important to investigate anti-forensics techniques. It not only checks the reliability of existing blind forensic methods, but also motivates us to investigate more robust forensic techniques. Up to now, several anti-forensics techniques are proposed to invalidate the passive image forensics of double JPEG compression (Stamm & Liu, 2010; Stamm & Liu, 2011), contrast enhancement (Cao & Liu, 2010; Kwok & Au, 2012), re-sampling (Kirchner & Böhme, 2008). In this paper, we propose an effective anti-forensics approach to fool the blind forensic of USM sharpening. As we know, there are only two state-of-the-art forensics approaches for USM sharpening in Cao and Liu (2009) and Cao and Liu (2011). The proposed anti-forensics approach is specifically designed to invalidate the forensics detection of USM sharpening by Cao and Liu (2009) and Cao and Liu (2011). The contribution of the proposed approach lies in the introduction of dithering noise to the overshoot images. It can remove both the overshoot artifacts and histogram artifacts, yet the same visual sharpening effect is still preserved as that of traditional sharpness. To the best of our knowledge, there is no similar anti-forensics work for USM sharpening in the existing literature.

Crime Simulation Using GIS and Artificial Intelligent Agents

Xuguang Wang, Lin Liu and John Eck (2008). *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems (pp. 209-225).*
www.igi-global.com/chapter/crime-simulation-using-gis-artificial/5265?camid=4v1a