An Improved Counter-Forensic Algorithm to Erase the JPEG Compression Artifacts

Guorui Sheng, LuDong University, Yantai, China
Bo Yang, Yantai Vocational College, Yantai, China

ABSTRACT

With the growing awareness of the fraud case for digital images, the researchers have developed some forensic techniques that based on the intrinsic statistical history or trace left by the jpeg compression to determine an image’s manipulation. Aiming at these forensic algorithms, special anti-forensic techniques was developed by removing footprints caused by jpeg compression. In this paper, the authors present an improved counter-forensic scheme that based on parameter adjustment. The simulation shows that by using the proposed strategy and combining the chaotic theory, the scheme can erase the quantization artifacts perfectly, even when the compression factor $Q \leq 50$.

Keywords: Anti-Forensics, Chaotic Signal, Counter Forensic Algorithm, Digital Image Forgery, JPEG Compression

INTRODUCTION

Nowadays digital images are playing an important role in people’s daily life, due to the popularity of low-cost and high resolution digital cameras, also the rapid expansion of high speed Internet. When people enjoy the entertainment brought by digital images, they also suffer from forgery images which has become a potential outbreak, because of the more and more powerful image editing software, with which digital images can be easily manipulated and altered without leaving visible footprints. The forged image may lead to serious social problem by rapid spread through Internet and mobile networks (Sugumaran, 2009), this has arouse wide academic interest, many forensic method have been developed to judge the authenticity and credibility of digital image.

The image forensic techniques includes two categories: proactive and passive forensics. For proactive forensics, special information such as watermark was embedded into original image in advance. Such information will be extracted and compared with original embedded information when checking the authenticity of an image. The main technique of proactive forensics is watermarking (Reyc, 2003; Potdar, 2003).
2005; Weng, 2013; Liu, 2010), which takes advantage of redundant information in digital images. Nowadays, some digital cameras support embedding watermark into digital image automatically when taking pictures. The main limitation of proactive forensic is that people usually can’t know which image should be checked in advance when facing large amounts of digital images. On the contrary, the passive forensics can judge the authenticity of an image without any embedded information in advance. The wide application of this kind of technique motivated many researchers focus on this domain.

As a mature standard for image compression, JPEG has been widely used. Most digital image is saved and transferred in JPEG form. Therefore, the intrinsic footprints left by the JPEG compression may give useful information for the inspector to trace the clues left by previous JPEG history. Some forensic algorithm have been proposed based on statistical feature caused by JPEG compression process: (Popescu, 2005) gave the evidence of if an image underwent double JPEG compression; (Lukas, 2003) proposed method which can estimate the primary quantization matrix; (Li, 2009) and (Sun, 2007) extracted block artifact grids (BAG) by employing the quantization artifact during JPEG processing. The mismatch between these grids can be used as footprints of tampering. We can conclude that if the original image and the corresponding tampered image are all coded in JPEG form, there must be obvious clues which can be used as forensic purposes.

Forensic methods are sure to face the challenge from attackers who will never stop attempting to make forensic methods lose efficacy. So the study of image anti-forensic techniques is also important, which can promotes the existing forensic methods to be more and more perfect and robust. There are already some anti-forensic achievements as following: (Kirchner, 2008) designed an operator to conceal the peak-gap artifacts which left in the histogram of the contrast-enhanced image; (Stamm, 2011) and (Stamm, 2010) hid the DCT coefficient quantization artifacts through adding anti-forensic dither. The method mentioned above can make most existing forensic methods aiming at JPEG images do not work well, but when these anti-forensic methods work, all coefficients in the high frequency sub-bands will most probably be quantized to zero, which will cause the parameter estimator has no solution. This can be clues to the forensic investigator.

In this paper, a novel image anti-forensic algorithm is proposed. This method can attack against the existing BAG-based forensic methods proposed by (Li, 2009) and (Ye, 2007), also different with stamm’s work (Stamm, 2011) and (Stamm, 2010), a chaos-based dither technology together with parameter adjustment is used, by mapping the chaotic noise into image’s DCT quantization coefficients with the purpose of removing artifacts. Compared with Stamm’s work (Stamm, 2011) and (Stamm, 2010), the proposed method perform better when the JPEG quality factor is much lower. The added chaotic noise can help to erase the quantization artifacts even when the compression factor \( Q \leq 50 \).

**BRIEF REVIEW OF THE JPEG COMPRESSION**

When an image with the size of \( I_{M \times N} \) is compressed in JPEG format, it must undergo two phases: encoding and decoding.

For the process of encoding, the image is first segmented into a series of non-overlapping sub-blocks with the size of \( 8 \times 8 \) pixels, denoting each sub-block as:

\[
B_{i,j}^k \begin{cases} 1 \leq i, j \leq 8, 1 \leq k \leq \left\lfloor \frac{M}{8} \times \frac{N}{8} \right\rfloor \end{cases}
\]

Then the 2D-DCT transform is applied to each sub-block \( B_{i,j}^k \). Each transformed DCT coefficient \( C_{i,j} \) is quantized by its corresponding quantizer \( Q_{i,j} \) within a quantization table \( Q \). It should be noted here that different digital device may have distinct quantization table.
Related Content

Definition and Analysis of a Fixed Mobile Convergent Architecture for Enterprise VoIP Services
[www.igi-global.com/article/definition-analysis-fixed-mobile-convergent/34069?camid=4v1a](www.igi-global.com/article/definition-analysis-fixed-mobile-convergent/34069?camid=4v1a)

Usability of CAPTCHA in Online Communities and Its Link to User Satisfaction
[www.igi-global.com/chapter/usability-of-captcha-in-online-communities-and-its-link-to-user-satisfaction/214742?camid=4v1a](www.igi-global.com/chapter/usability-of-captcha-in-online-communities-and-its-link-to-user-satisfaction/214742?camid=4v1a)
Micro to Macro Social Connectedness Through Mobile Phone Engagement
www.igi-global.com/chapter/micro-to-macro-social-connectedness-through-mobile-phone-engagement/214676?camid=4v1a

Illustration of Centralized Command and Control for Flocking Behavior
www.igi-global.com/article/illustration-of-centralized-command-and-control-for-flocking-behavior/124957?camid=4v1a