A JPEG blocking artifact detector for image forensics

Dinesh Bhardwaj, Vinod Pankajakshan

PII: S0923-5965(18)30206-6
DOI: https://doi.org/10.1016/j.image.2018.07.011
Reference: IMAGE 15426

To appear in: *Signal Processing: Image Communication*

Received date : 4 March 2018
Revised date : 21 June 2018
Accepted date : 31 July 2018

A JPEG Blocking Artifact Detector for Image Forensics

Dinesh Bhardwaj*, Vinod Pankajakshan

Department of Electronics & Communication Engineering, Indian Institute of Technology Roorkee, Roorkee 247667, India

Abstract

Detection of JPEG blocking artifacts in an image plays an important role in the forensic analysis. JPEG anti-forensic techniques try to remove these artifacts to disguise forensic detectors. This paper proposes a new technique for detecting JPEG blocking artifacts. Unlike in uncompressed images, when a JPEG compressed image is cropped, there is a change in the inter-block correlation of DCT coefficients due to the shifting of blocking artifacts. We propose to use this change in correlation to detect the blockiness in an image. Experiments conducted on a large set of images show that the proposed detector outperforms the existing detectors in detecting blocking artifacts in anti-forensically modified images.

Keywords: Blocking artifacts , image forensics, JPEG compression

1. Introduction

JPEG is the most commonly used image compression standard. There are mainly two characteristic traces of JPEG compression, *blocking artifacts* and *quantization artifacts*, which are exploited in forensic analysis. In JPEG encoding, a given image is divided into non-overlapping blocks of size 8 × 8 pixels and each block is transform-coded independently. Due to the independent encoding of the blocks, pixel discontinuities are introduced across block boundaries of the decompressed image. This results in *blockiness* in the decompressed image, known as the JPEG blocking artifacts [1]. Quantization artifacts are generated by the quantization step in transform coding. If the image undergoes single JPEG compressions, the coefficient values in each DCT subband are clustered around integer multiples of the corresponding quantization step size. This results in a comb-like pattern in the DCT subband histograms. If the image undergoes multiple JPEG compressions, periodic patterns specific to the quality factors of individual compression are introduced in the DCT subband histograms [2]. The blocking artifacts in an image can be detected [1, 3] and used as an indication of the presence of JPEG compression. Luo et al. [4] exploited blocking artifacts for tampering detection by computing a blocking artifact characteristics matrix (BACM). The quantization artifacts are mainly exploited for quantization table estimation [1, 5] and image splicing detection [2, 6].

Stamm et al. [7] pioneered the research in JPEG anti-forensics. First, they proposed an anti-forensic dither to hide the quantization artifacts and later they incorporated a deblocking step to remove blocking artifacts [8]. The anti-forensic technique was able to defeat all the then existing JPEG forensic detectors. An anti-forensic scheme based on Shrink and Zoom (SAZ) is proposed by Sutthiwan et al. [9] to mislead double JPEG compression detectors. Barni et al. [10] proposed a universal anti-forensic technique capable of misleading multiple-JPEG compression detectors. In this method, the DCT subband histograms of a multiple-compressed image are remapped such that the resulting histograms resemble those of a single compressed image. Fan et al. [11] proposed a JPEG anti-forensic algorithm with the objective of improving the perceptual quality of the anti-forensically modified image while maintaining forensic undetectability. This method consists of four steps: first round total variation (TV) based deblocking, addition of perceptual dither in the DCT domain, second round TV-based deblocking and finally the decalibration. The method proposed in [12] targets detectors based on the distribution of the first significant digit (FSD) of the DCT coefficients. This method can be used to restore the FSD distribution of either a single/double compressed image to that of an uncompressed image or a double compressed image to that of a single compressed image.

The introduction of anti-forensic techniques prompted the research on the methods for countering anti-forensics. Lai et al. [13] and Valenzise et al. [14] proposed methods for countering Stamm et al.'s [7] anti-forensic technique. In [13], two different kinds of detectors for anti-forensically modified images are proposed. The first detector exploits the fact that the anti-forensic operation does not modify high-frequency DCT subbands. The second detector exploits the difference between the variance in DCT co-

*Corresponding author

Email addresses: dinesdec@iitr.ac.in (Dinesh Bhardwaj), vinodfec@iitr.ac.in (Vinod Pankajakshan)