Accepted Manuscript

A novel contrast enhancement forensics based on convolutional neural networks

Jee-Young Sun, Seung-Wook Kim, Sang-Won Lee, Sung-Jea Ko

PII: S0923-5965(18)30103-6
DOI: https://doi.org/10.1016/j.image.2018.02.001
Reference: IMAGE 15328

To appear in: *Signal Processing: Image Communication*

Received date : 27 September 2017
Revised date : 11 January 2018
Accepted date : 1 February 2018

Please cite this article as: J.-Y. Sun, S.-W. Kim, S.-W. Lee, S.-J. Ko, A novel contrast enhancement forensics based on convolutional neural networks, *Signal Processing: Image Communication* (2018), https://doi.org/10.1016/j.image.2018.02.001

A Novel Contrast Enhancement Forensics Based on Convolutional Neural Networks

Jee-Young Sun[a], Seung-Wook Kim[a], Sang-Won Lee[a], Sung-Jea Ko[a]*

[a]*Department of Electrical Engineering, Korea University, Anam-ro 145, Seongbuk-gu, Seoul, 02481 Republic of Korea*

{jysun,swkim,swlee}@dali.korea.ac.kr

**Corresponding author; sjko@korea.ac.kr*

Abstract

Contrast enhancement (CE), one of the most popular digital image retouching technologies, is frequently utilized for malicious purposes. As a consequence, verifying the authenticity of digital images in CE forensics has recently drawn significant attention. Current CE forensic methods can be performed using relatively simple handcrafted features based on first-and second-order statistics, but these methods have encountered difficulties in detecting modern counter-forensic attacks. In this paper, we present a novel CE forensic method based on convolutional neural network (CNN). To the best of our knowledge, this is the first work that applies CNN to CE forensics. Unlike the conventional CNN in other research fields that generally accepts the original image as its input, in the proposed method, we feed the CNN with the gray-level co-occurrence matrix (GLCM) which contains traceable features for CE forensics, and is always of the same size, even for input images of different resolutions. By learning the hierarchical feature representations and optimizing the classification results, the proposed CNN can extract a variety of appropriate features to detect the manipulation. The performance of the proposed method is compared to that of three conventional forensic methods. The comparative evaluation is conducted within a dataset consisting of unaltered images, contrast-enhanced images, and counter-forensically attacked images. The experimental results indicate that the proposed method outperforms conventional forensic methods in terms of forgery-detection accuracy, especially in dealing with counter-forensic attacks.

Keyword

Digital image forensics, contrast enhancement, convolutional neural networks, deep learning, gray level co-occurrence matrix.

1. Introduction

As image and video editing techniques rapidly develop, image manipulation has become an easy process that can be exploited for malicious purposes, such as copyright infringement, and spreading false information in the news media or litigation. In recent years, various digital forensic methods have been proposed to verify the authenticity of multimedia data. Digital image forensics identifies traceable statistical artifacts left behind after an image alteration and distinguishes forgeries from unaltered images. In general, image manipulation leaves unique fingerprints on images; thus, most digital image forensic methods focus on detecting different types of image manipulations, which are broadly divided into two categories: 1) content-preserving operations including resampling [1], compression [2], median filtering [3,4], and contrast enhancement (CE) [5–7]; and 2) content-changing operations, such as splicing and copy-move manipulation [8–10]. Although the content-preserving operations may not pertain to malicious image tampering, detecting these alteration is still forensically significant. Especially, the detection of the globally applied CE manipulation can provide insight into the processing history of an image [5]. Furthermore, since CE is frequently employed to disguise the evidence of image tampering, detecting such a manipulation can provide useful prior information in the identification of content-changing operations. Thus, this paper focus on the development of a forensic method of detecting the CE manipulation.

*This work was supported by the ICT R&D program of MSIP/IITP [B2014-0-00077, Development of global multi-target tracking and event prediction techniques based on real-time large-scale video analysis]

*This paper has supplementary downloadable material available at http://doi.org/10.6084/m9.figshare.5160982.v1, provided by the authors. This includes .mat format dataset and .py format source codes for training and testing the proposed CNN for contrast enhancement forensics.