Digital Investigation 8 (2012) 215–225

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Digital image forgery detection and estimation by exploring basic image manipulations

S. Devi Mahalakshmi [a,*], K. Vijayalakshmi [b], S. Priyadharsini [a]

[a] Computer Science and Engineering Department, Mepco Schlenk Engineering College, Mepco Engineering College (PO), Sivakasi 626005, Virudhunagar, Tamilnadu, India

[b] Information Technology Department, Mepco Schlenk Engineering College, Sivakasi 626005, India

ARTICLE INFO

Article history:
Received 8 June 2011
Accepted 19 June 2011

Keywords:
Digital forensics
Digital image forgery
Fake image
Interpolation
Rescaling
Rotation
Contrast enhancement
Histogram equalization

ABSTRACT

In this modern age in which we are living, digital images play a vital role in many application areas. But at the same time the image retouching techniques has also increased which forms a serious threat to the security of digital images. To cope with this problem, the field of digital forensics and investigation has emerged and provided some trust in digital images. In this paper we proposed a technique for image authentication that detects the manipulations that are done in the digital images. In most of the image forgeries such as copy-and-paste forgery, region duplication forgery, image splicing forgery etc basic image operations or manipulations are often involved. Thus if there exists the evidence for basic image alterations in digital images we can say that the image has been altered. This paper aims at detecting the basic image operations such as re-sampling (rotation, rescaling), contrast enhancement and histogram equalization which are often done in forged images. The available interpolation related spectral signature method is used for detecting rotation and rescaling and for estimating parameters such as rotation angle and rescale factors. This rotation/rescaling detection method detects some unaltered images as altered one when the images are JPEG compressed. We have overcome that problem by adding noise in the input images. We have also used the existing fingerprint detection technique for detecting contrast enhancement and histogram equalization. Besides the techniques discussed in the existing method, we identified a unique property for histogram equalization which can help us to differentiate contrast enhancement from histogram equalization. This work is tested in USC-SIPI database which consists of general unaltered images and achieved results with satisfactory accuracy.

1. Introduction

Digital image forgery is the process of manipulating the original photographic images to create the forged image. Digital forensics aims to detect the alterations done in the images by investigating the images. With the usage of powerful image editing tools such as Paint, Photoshop etc, numerous image retouching techniques have become practical. Fake images are sometimes created for amusements and advertisements such as a cat playing guitar, baby smoking cigarette. These fake images used in harmless environments are not bad. But at the same time, malicious alteration of image content forms a serious threat to the security of digital images. Digital images used in law and order places should be genuine and so the image forgery detection techniques play a major role in these places.

The fake or forged images are created with the aim of altering the information present in the original images. In most of the forged images basic image operations such as rotation, rescaling, stretching, zooming, and enhancing

* Corresponding author. Tel.: +91 9942349553.
E-mail address: sdevi@mepcoeng.ac.in (S. Devi Mahalakshmi).

1742-2876/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2011.06.004

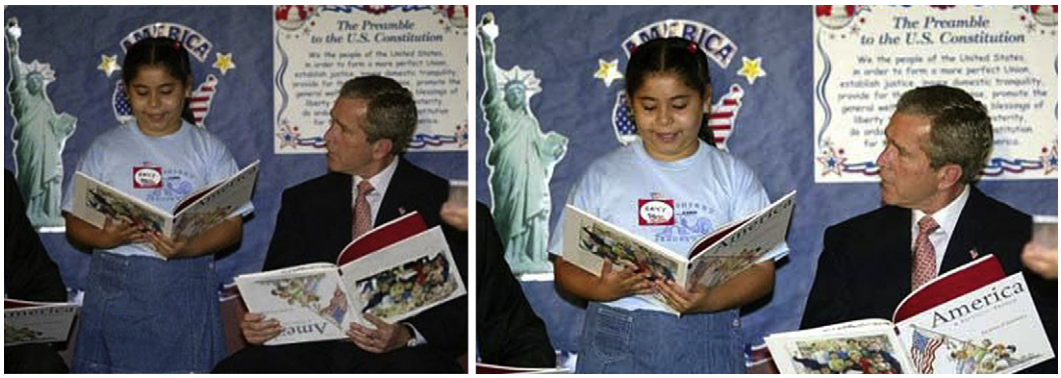

Fig. 1. The fake image (left) showing George Bush holding the book upside down at a school and its original one (right).

contrast are often involved. In many applications there is the need to detect whether the image has been retouched or not instead of detecting which type of forgery is involved. In such cases our detection method can be used as it detects the basic image alterations performed in the digital images. Consider a copy-and-paste forgery. In this forgery, an image region is copied from image and pasted either in the same or different image. To make the copied region fit in the original image and to make the forged image look natural the image manipulations are performed. Therefore detecting the image manipulations discussed in our proposed technique is still forensically significant.

Fig. 1 shows an example for fake image generated in real life and its original one. In 2002, this fake photograph was widely circulated to show President George Walker Bush holding a children's book upside down during a photo opportunity at a grade school. Seasoned photo experts, however, noticed that the photo on the back of the book Bush is holding is a left-to-right mirror image of the one that the girl is holding, and proved that it had been photo manipulated. Nonetheless, the picture was and continues to be cited as evidence of the former president's supposed lack of intelligence.

Fig. 2 shows another example for the fake image and its original one. In September 2010, Egypt's largest newspaper, the state-run Al-Ahram, showed a forged photo of world leaders walking the red carpet during Middle East peace talks at the White House. It was notable in that Egyptian President Hosni Mubarak is leading the way, ahead of even President Barack Obama in his own residence. It didn't take long for observers to figure out the Al-Ahram photo was an alteration. Not only the floor and the rest of the background are awkwardly cropped out, making it appears as if the leaders are walking on a flying carpet, and there are clearly visible borders around Mubarak where he'd been repositioned in front of Obama and Palestinian Authority President Mahmoud Abbas.

This paper is organized as follows: Section 2 describes about the existing works for image forgery detection and their limitations. Section 3 explains the methodology of our proposed system. Section 4 discusses about the results of the proposed system and also discusses the detection performance of the proposed system followed by conclusion and future work provided in Section 5.

2. Related works

In recent years, many image forgery detection techniques have been proposed and we have surveyed some of the existing methodologies for forgery detection here. The existing approaches can be classified into two categories: Active or Non-blind approach and Passive or Blind approach.

Active forgery detection techniques require prior knowledge about the original image such as a reference template, or features extracted from the original. Therefore they are not automatic. These methods have limited values in applications since the original image is unavailable in

Fig. 2. The fake image (left) of World Leaders in the White House and its original one (right).