Università degli Studi Firenze

Scuola di Ingegneria

Corso di Laurea in Ingegneria Informatica

Image splicing detection with local illuminant estimation

Candidato

Lorenzo Cioni

Relatore

Prof. Alessandro Piva

Correlatori

Prof. Carlo Colombo

Dott. Massimo Iuliani

Dott. Marco Fanfani

Anno Accademico 2015/2016

Dedica

Contents

Introduction

Recently advanced image processing tools and computer graphics techniques make it straightforward to edit or modify digital images. In a forensics scenario, this raises the challenge of discriminating original images from malicious forgeries. Particular region from an image is pasted into other image with purpose to create image splicing.

Image splicing is a common type of image tampering (manipulation) operation. The image integrity verification as well as identifying the areas of tampering on images without need to any expert support or manual process or prior knowledge original image contents is now days becoming the challenging research problem.

Investigating image's lighting is one of the most common approaches for splicing detection. This approach is particularly robust since it's really hard to preserve the consistency of the lighting environment while creating an image composite (i.e. a splicing forgery).

In this scenario, there are mainly two main approaches:

1. based on the object-light geometric arrangement
2. based on illuminant colors

We focused our attention on the illuminant-based approach, which assumes that a scene is lit by the same light source. More light sources are admitted but far enough such as to produce a constant brightness across the image. In this condition, pristine images will show a coherent illuminant representation; on the other hand, inconsistencies among illuminant maps will be exploited for splicing detection.

Illuminant Maps locally describes the lighting in a small region of the image. In the computer vision literature exists many different approaches for determining the illuminant of an image has been proposed. In particular, such techniques are divided into two main groups: statistical-based and physics-based approaches.

Regarding the first group, we start investigating on the *Grey-World algorithm* [1], which is based on the Grey-World assumption, i.e. the average reflectance in a scene is achromatic. In [3], this algorithm proved to be special instances of the Minkowski-norm. Van de Weijer et al. [7] than proposed an extension of the Gray-World assumption, called *Gray-Edge hypothesis* [7], which assumes that the average of the reflectance differences in a scene is achromatic. The reflectance differences can be determined by taking derivatives of the image. Therefore, the authors present a framework with which many different algorithms can be constructed. We focus our attention on the last case, called generalized *Grey-World algorithm (GGE)*. The resulting illuminant maps presents also global illuminant features because of the gray-world and grey-edge assumptions.

For the latter group, was investigate the method proposed by Riess et al. [4], which extends the *Inverse Intense Chromaticity* (*IIC*) space approach proposed by Tan et al. [5] and tries to model the illuminants considering the dichromatic reflection model [6]. In this case, the illuminant map is evaluated dividing images into blocks, named superpixels, of approximately the same object color, then the illuminant color is evaluated for each block solving the lighting models locally.

Carvalho et al. [2] then presents a method that relies on a combination of the two approaches for the detection of manipulations on images containing human faces. In addition to maps, a large set of shape and texture descriptors are used together. Note that, from a theoretical viewpoint, it is advantageous to consider only image regions that consist of approximately the same underlying material:

for this reason, in [2] the authors focused their analysis on human faces.

In [2] it is also shown that the difference between the two maps, GGE and IIC, increased when fake images are processed. This insight leads to the idea that it is possible to localize tampered image regions simply by considering IM differences with some metric, avoiding the computation of multiple descriptors.

Chapter 1

Related work

1.1 Image splicing

Images and videos have become the main information carriers in the digital era and used to store real world events. The significant possible of visual media and the no difficulty in their acquisition, division and storage is such that they are more and more exploited to convey information. But digital images are easy to manipulate because of the availability of the powerful editing software and sophisticated digital cameras.

Image processing experts can easily access and modify image content and therefore its meaning without leaving visually detectable traces. Moreover, with the spread of low-cost user friendly editing tools the art of tampering and counterfeiting visual content is no more restricted to experts. As a result, the manipulation of images for malicious purposes is now more common than ever.

At the start, the manipulation is just improve the image's performance, but then many people started to change the image's content, even to gain their ends by these illegal and immorality methods. Based on the above reasons, it is important to develop a credible method to detect whether a digital image is tempered, so-called digital image forgery.

Digital imaging resulted into many real life benefits, but at same side it's vulnerable to many threats of crimes. To check whether image is real or forged? , it is very difficult task. In fact, the security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. These techniques can be divided into two major groups: intrusive and non-intrusive. In intrusive (active) techniques, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and authenticity is established by verifying if the true signature matches the retrieved signature from the test image [3] [4] [5]. This approach is limited due to the inability of many digital cameras and video recorders available in the market to embed extrinsic fingerprints [6]. Further the drawbacks of intrusive methods used as motivation for non-intrusive method [6] in order to validate the authenticity of digital images. These techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. There are many challenges in blind techniques, for instance, reducing false positive rates (i.e., an authentic image being detected as a forged image), making the system fully automated, localizing the forgery, detecting forgery of any type of image format (compressed or uncompressed), increasing the robustness and reliability, etc. Image splicing is to create a new image from two or more images, and it is far and wide used for image forgery. Image splicing detection is a main difficulty in image forensics. However there are very hardly any solutions to this problem .An given below example of a digital forgery is shown in Figure 1. As the newspaper cutout shows, three different photographs were used in creating the composite image: Image of the White House, Bill Clinton, and Saddam Hussein. The White House was rescaled and blurred to create an illusion of an out-of-focus background. Then, Bill Clinton and Saddam were cut off from two different images and pasted on the White House image. Care was taken to bring in the speaker stands with microphones while preserving the correct shadows and lighting. Fig. 1 is, in fact, an example of a very realistic looking forgery.

1.2 Methods based on light inconsistencies

Chapter 2

Splicing detection using local illuminant estimation

2.1 Background theory

2.1.1 Illuminant maps

Riess work

Generalized Greyworld algorithm

Inverse Intensitiy Chromaticiy

2.2 Proposed approach

2.2.1 Overview

2.2.2 Face splicing detection module

Descrizione della tecnica

2.2.3 Region splicing detection module

Descrizione della tecnica

Chapter 3

Experiments and results

3.1 Evaluation datasets

Overview

3.1.1 Columbia

3.1.2 DSO-1

3.1.3 DSI-1

3.1.4 NIMBLE

3.2 Performance

Conclusions

Bibliography

[1] G. Buchsbaum. A spatial processor model for object colour perception. *Journal of the Franklin Institute*, 310(1):1 – 26, 1980.

[2] T. Carvalho, F. A. Faria, H. Pedrini, R. d. S. Torres, and A. Rocha. Illuminant-based transformed spaces for image forensics. *IEEE Transactions on Information Forensics and Security*, 11(4):720–733, 2016.

[3] G. D. Finlayson and E. Trezzi. Shades of gray and colour constancy. In *Color and Imaging Conference*, volume 2004, pages 37–41. Society for Imaging Science and Technology, 2004.

[4] C. Riess and E. Angelopoulou. Scene illumination as an indicator of image manipulation. In *International Workshop on Information Hiding*, pages 66–80. Springer, 2010.

[5] R. T. Tan, K. Nishino, and K. Ikeuchi. Color constancy through inverse-intensity chromaticity space. *JOSA A*, 21(3):321–334, 2004.

[6] S. Tominaga and B. A. Wandell. Standard surface-reflectance model and illuminant estimation. *JOSA A*, 6(4):576–584, 1989.

[7] J. Van De Weijer, T. Gevers, and A. Gijsenij. Edge-based color constancy. *IEEE Transactions on image processing*, 16(9):2207–2214, 2007.

Ringraziamenti