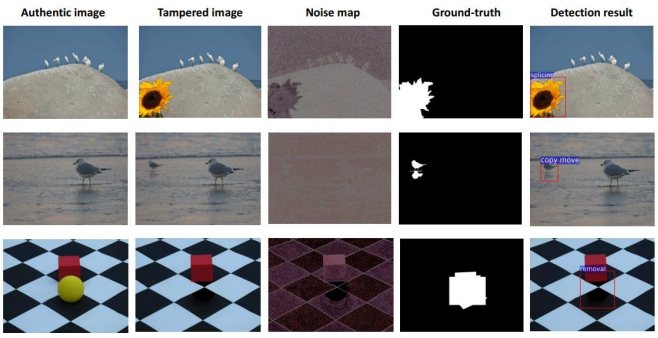
Photo fakery nabbed via outsmarting techniques

25 June 2018, by Nancy Owano



Qualitative results for multi-class image manipulation detection on NIST16 dataset. RGB and noise map provide different information for splicing, copy-move and removal. By combining the features from the RGB image with the noise features, RGB-N produces the correct classification for different tamepring techniques. Credit: Peng Zhou et al.

Adobe Research has been getting busy nailing down how to spot image manipulations by unleashing AI on the case. In doing so, they may be achieving real headway in the field of image forensics.

You can check out the paper, "Learning Rich Features for Image Manipulation Detection," by authors whose affiliations include Adobe Research and University of Maryland, College Park.

The paper should be seen by fakers who think they can get away with flaunting their tricks because Adobe's scientists are eager to get and stay on your case.

Senior research scientist Vlad Morariu, for example, set out on a quest to solve the problem on how to detect images that have been subject to tampering. Morariu is no stranger to the task. In 2016, he took up a challenge of detecting image manipulation as part of the DARPA Media Forensics program.

How can you detect if a picture is authentic or has been manipulated?

In this case, he and his colleagues watched out for manipulation via three types of operations. Splicing [parts of two different images are combined], cloning [when you move an object from one pace to another] and removal. [In the latter, you remove an object—and the space can be filled in.]

First, let's hear some noise.

"Every image has it own imperceptible noise statistics. When you manipulate an image, you actually move the noise statistics along with the content. "

A posting in the Adobe Blog also carried his remarks about what we can know about manipulation. "File formats contain metadata that can be used to store information about how the image was captured and manipulated. Forensic tools can be used to detect manipulation by examining the noise distribution, strong edges, lighting and other pixel values of a photo. Watermarks can be used to establish original creation of an image."

Even though the human eye may be unable to spot the artifacts, detection is possible by close analysis at the pixel level, said Adobe, or by applying filters that help highlight changes. Not all such tools, however, work perfectly to discover tampering.

Enter artificial intelligence and machine learning—and they entered Vlad's head, as potentially reliable paths to identify a modified image.

Can AI not only spot manipulation but also identify the type of manipulation used and highlight the specific area of the photograph that was altered?

To get answers, he and team trained a deep learning neural network to recognize image manipulation.

Two techniques were tried, (1) an RGB stream (changes to red, green and blue color values of pixels) to detect tampering and (2) use of a noise stream filter.

Results? The authors said in their paper that "Experiments on standard datasets show that our method not only detects tampering artifacts but also distinguishes between various tampering techniques. More features, including JPEG compression, will be explored in the future."

The Adobe Blog reminds us that digital image manipulation is a technology that "can be used for both the best and the worst of our imaginations."

Why this research matters: Techniques used provide more possibility and more options for managing the impact of digital manipulation, and they potentially answer questions of authenticity more effectively, said the Adobe Blog.

Paul Lilly weighed in at *HotHardware*: "It's not a perfect system, but it's nice to see companies like Adobe working on ways to separate fact from fiction in photography."

More information: Learning Rich Features for Image Manipulation Detection, openaccess.thecvf.com/content_ … _CVPR_2018_paper.pdf

Abstract
Image manipulation detection is different from traditional semantic object detection because it pays more attention to tampering artifacts than to image content, which suggests that richer features need to be learned. We propose a two-stream Faster R-CNN network and train it endto-end to detect the tampered regions given a manipulated image. One of the two streams is an RGB stream whose purpose is to extract features from the RGB image input to find tampering artifacts like strong contrast difference, unnatural tampered boundaries, and so on. The other is a noise stream that leverages the noise features extracted from a steganalysis rich model filter layer to discover the noise inconsistency between authentic and tampered regions. We then fuse features from the two streams through a bilinear pooling layer to further incorporate spatial co-occurrence of these two modalities. Experiments on four standard image manipulation datasets demonstrate that our two-stream framework outperforms each individual stream, and also achieves state-of-the-art performance compared to alternative methods with robustness to resizing and compression.

APA citation: Photo fakery nabbed via outsmarting techniques (2018, June 25) retrieved 22 October 2021 from https://techxplore.com/news/2018-06-photo-fakery-nabbed-outsmarting-techniques.html