Image Forensics Project
ECE 278: Fall 2017

B.S. Manjunath
manj@ucsb.edu

November 12, 2019

Introduction

Even before "fake news" became a daily news item, "fake images" have influenced both science and politics. In early 2000s, the journal Science had to withdraw a high-profile paper on cloning after it was discovered that the images published were all manipulated! In another instance, a news article from a foreign country showed off four ballistic missiles being fired: the problem was that there were no four missiles but cut and pasted pictures being shown. In both instances, images were copied and manipulated, and if it were not for some careful "viewing", the manipulations would not have been discovered. In 2016, DARPA started the MediFOR (Media Forensics) program to investigate image/video manipulations.

Given the vast number of image processing techniques, which of these constitute image manipulation will always remain subjective. In fact, if we define any modification of the image sensor output as tampering, then the majority of digital images we use would be considered inauthentic. Repeated resampling and JPEG compression of an entire image may be an attempt to cover up some modification artifact, or the result of an image being posted and downloaded from several different social media sites. The demand for higher quality images from smaller and cheaper mobile cameras has also led to significant post-processing without the user's knowledge. Modern cellphone cameras have been shown to correct for lens distortion in software, by resampling the sensor output to more precisely match the pinhole camera model [13]. Apple's High Dynamic Range (HDR) mode takes images at several different exposure levels, and blends them to produce an image with contrast in both light and dark areas.

In most cases, we would like to know not only if an image manipulated, but how and where it was modified. For this project, we will consider only copy-paste manipulations with resampling. For many natural images, the object scales may be quite different. Therefore the object being spliced into the target image must be resampled differently than the background. A common approach is to detect these differences in resampling factors for small patches to localize the spliced region.

For simplicity, you may assume the following for this project:

- There will be at most one region which has been copy-pasted.
- There will be untampered images in the dataset, for which you should return no mask.
- You need to separate the two regions, but you do not need to say which region is the copy-pasted one. It should be visually apparent from your mask output that one of the objects does not belong.
- There will always be some level of resampling done on the pasted region. Further, only nearest-neighbor and bilinear interpolation will be used.

Development and test datasets will be made available for this project, each containing 10 images. The development images will be released soon after this project is posted, and you must include results on these images in your final report. The test images will be held out until some time before the final presentations.

Helpful Publications

1. Kirchner, Matthias. "Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue." Proceedings of the 10th ACM workshop on Multimedia and security. ACM, 2008.
   `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.174.2972&rep=rep1&type=pdf`

2. Popescu, Alin C., and Hany Farid. "Exposing digital forgeries by detecting traces of resampling." IEEE Transactions on signal processing 53.2 (2005): 758-767.
   `https://farid.berkeley.edu/downloads/publications/sp05.pdf`

3. Vzquez-Padn, David, Pedro Comesana, and Fernando Prez-Gonzlez. "An SVD approach to forensic image resampling detection." 2015 23rd European Signal Processing Conference (EUSIPCO). IEEE, 2015.
   `https://ieeexplore.ieee.org/document/7362748`

Project Presentation: In class, Thursday, December 5 and Friday, December 6

We will have two days for presentations. As there are around 20 groups and less than 4 total hours of class time, each group will have 8 minutes to present. Your presentation should include results on all 10 test images, followed by an explanation of your method.

Project Report and code: Due Saturday, Dec 7, 12 noon (online submission)

The project report is free-form, this being a graduate class. Make sure that you emphasize all of the critical pieces and adequately address all the issues above. Include results of your method on the 10 images provided for development.

References

1. DARPA MEDIFOR project: `https://www.darpa.mil/program/media-forensics`

2. IEEE IFS-TC Image Forensics Challenge: `http://ifc.recod.ic.unicamp.br/fc.website/index.py?sec=5`. This site has 400 tampered and 400 untampered images that you can work with in developing your methods.

3. This is a link to some MATLAB code implementing a few forensics methods. `https://github.com/MKLab-ITI/image-forensics`

4. This paper and associated code describes and implements a well know strategy to detect manipulations. Typically one would move regions from part of the image to cover up or duplicate objects (as in the missile example mentioned above). This work won a previous forgery detection competition. `http://www.grip.unina.it/research/83-image-forensics/90-copy-move-forgery.html`

5. H. Farid, "Image forgery detection" Signal Processing Magazine, IEEE, 26, no. 2 (2009): 16-25.

6. J.A. Redi, W. Taktak, and Jean-Luc Dugelay. "Digital image forensics: a booklet for beginners," Multimedia Tools and Applications 51, no. 1 (2011): 133-162."

7. A. Piva. "An overview on image forensics," ISRN Signal Processing 2013 (2013).

8. L. Nataraj, A. Sarkar and B. S. Manjunath, "Improving re-sampling detection by adding noise," Proceedings of SPIE, 2010, Media Forensics and Security, vol. 7541, pp. 75410I-75410I-11, Jan. 2010.

9. L. Nataraj, A. Sarkar and B. S. Manjunath, "Adding Gaussian Noise to Denoise JPEG for detecting Image Resizing," IEEE International Conference on Image Processing, 2009, pp. 1493-1496, Cairo, Egypt, Nov. 2009.

10. A. Sarkar, L. Nataraj and B. S. Manjunath, "Detection of Seam Carving and Localization of Seam Insertions in Digital Images," 11th ACM Workshop on Multimedia and Security, pp. 107-116, Princeton, New Jersey, Sep. 2009.

11. J. Bunk, J.H. Bappy, T. Mohammed, L. Nataraj, A. Flenner, B.S. Manjunath, S. Chandrasekaran, A.K Roy-Chowdhury, L. Peterson, "Detection and Localization of Image Forgeries using Resampling Features and Deep Learning," CVPR Workshop on Image Forensics, Hawaai, July 2017.
`https://escholarship.org/uc/item/8nk9629z`

12. Jawadul H. Bappy, Amit K. Roy-Chowdhury, Jason Bunk, Lakshmanan Nataraj, B. S. Manjunath, "Exploiting Spatial Structure for Localizing Manipulated Image Regions," The IEEE International Conference on Computer Vision (ICCV), 2017, pp. 4970-4979, Venice, October 2017.
`http://openaccess.thecvf.com/content_iccv_2017/html/Bappy_Exploiting_Spatial_Structure_ICCV_2017_paper.html`

13. Goljan, M. and Fridrich, J., "Sensor-fingerprint based identification of images corrected for lens distortion." In Media Watermarking, Security, and Forensics 2012 (Vol. 8303, p. 83030H). International Society for Optics and Photonics.
`http://www.ws.binghamton.edu/fridrich/Research/lens-distortion-12.pdf`

14. J.H. Bappy, C. Simons, L. Nataraj, B.S. Manjunath, A.K. Roy-Chowdhury, "Hybrid LSTM and Encoder-Decoder Architecture for Detection of Image Forgeries," IEEE Transactions on Image Processing (TIP), 2019
`https://intra.ece.ucr.edu/~mbappy/pubs/TIP_img_forgery.pdf`