Image Manipulation Detection using Computer Vision Methods

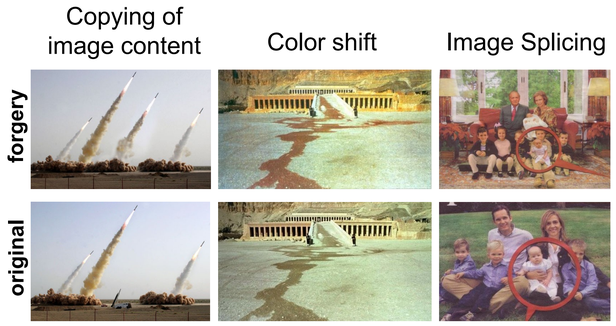
Christian Riess, Johannes Jordan, Elli Angelopoulou
{riess, jordan, elli}@i5.informatik.uni-erlangen.de, http://www5.informatik.uni-erlangen.de
Pattern Recognition Lab, University of Erlangen-Nuremberg, Germany

Friedrich-Alexander-Universität Erlangen-Nürnberg

LEHRSTUHL FÜR MUSTER-ERKENNUNG

Introduction

The detection of image manipulations is becoming a growing concern of journalism and law enforcement agencies



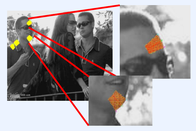
Source: http://www.rhetorik.ch/Bildmanipulation/Bildmanipulation.html

Common Approaches

- Verification of image sensing artifacts
  - Sensor noise fingerprinting
  - Lateral chromatic aberration
  - Bayer pattern identification

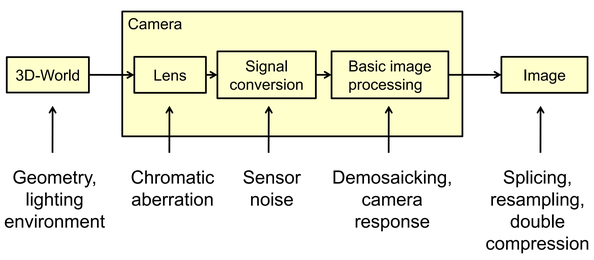
- Detection of traces of particular tampering operations
  - JPEG compression inconsistencies
  - Copy-move artifacts
  - Resampling artifacts

- Verification of scene consistency
  - Illumination direction
  - Illumination color



Detection Hooks

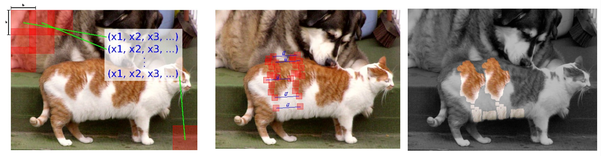
Manipulations leave traces in different steps of the image formation process



Methods on Output Image Artifacts

Copy-Move Forgery Detection (CMFD)

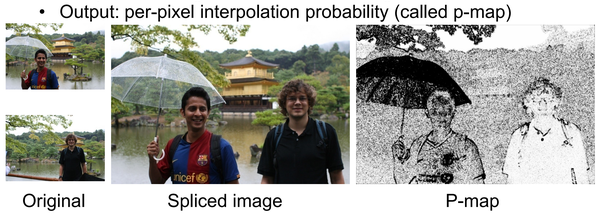
- Content is copied within the same image
- General approach (e.g. [1, 2, 3, 4]):
  - Extract local features
  - Match features
  - Copied area = sufficiently many matches align in an affine transform



- 20+ CMFD variants have been proposed
- Benchmark: **Image Manipulation Dataset** [5], most versatile and challenging available database

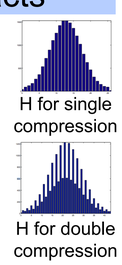
Splicing Detection: Resampling

- Spliced image parts are often scaled or rotated
- Rotation/scaling is typically done by interpolation
- Estimate interpolation parameters from the image
- General approach [6]:
  - Interpolation is approximated by a linear system of equations
  - Interpolation weights are estimated using EM
  - Output: per-pixel interpolation probability (called p-map)



Exploitation of JPEG-Artifacts

- Assume double compression with compression matrices Q and Q'
- Histogram H of a DCT coefficient j over many JPEG-blocks is then $H = \lfloor \lfloor \mathrm{DCT}_j(I)/Q_j \rfloor \cdot Q_j/Q'_j \rfloor$
- Double integer division leads to undulating values in H [7]



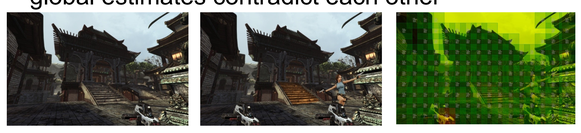
CV-BasedMethods

Towards Scene Decomposition

- Many early image forensics methods are inspired by related fields, e.g. steganography
- Especially for the verification of image sensing artifacts, thrilling results have been presented
- However, there is not a “one fits all” method to detect image forgeries
- Computer Vision methods play a key role in consistency checks on the image formation process and scene analysis
- Here, the most ambitious goal is to decompose the shown 3D-world in physically connected, interacting objects

Lateral Chromatic Aberration

- Image splicing disturbs the pattern of chromatic aberration
- Misregistration between the color channels can be estimated with a linear or polynomial model [8,9]
- Perform this estimation locally and globally
- An image is assumed to be tampered if local and global estimates contradict each other



Illumination Direction

- Illumination direction on spliced objects is very likely to differ
- Intensity distribution on object boundary allows to obtain the lighting direction in spherical coordinates
- The estimation can be done by solving a linear system of equations [10]

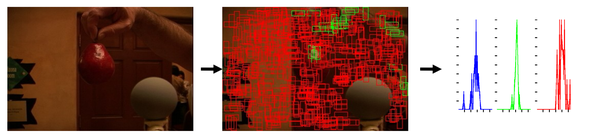
[1] S. Ryu, M. Lee, H. Lee: *Detection of Copy-Rotate-Move Forgery using Zernike Moments*, IH 2010.
[2] S. Bravo-Solorio, A. Nandi: *Passive Forensic Method for Detecting Duplicated Regions Affected by Reflection, Rotation and Scaling*, SPC 2009.

Illumination Consistency

- Light color and scene geometry must match [11]
- Estimate illuminant color locally
- Visualize transition between dominant illuminants in illuminant map and distance map
- Illuminant color estimation is ill-posed: Physics-based model allows outlier detection

Illuminant color estimation algorithm

- Segment image by chromaticity
- Within one such segment, draw local patches
- Project the pixels of a patch in Inverse Intensity-Chromaticity Space [12] and obtain an illuminant estimate.
- The segment illuminant color is a consensus of the per-patch estimates



[3] S. Bayram, H. Sencar, N. Memon: *An Efficient and Robust Method for Detecting Copy-Move Forgery*, ICASSP 2009.
[4] V. Christlein, C. Riess, E. Angelopoulou: *On Rotation-Invariance in Copy-Move Forgery*, WIFS 2010.
[5] C. Riess, J. Jordan, E. Angelopoulou: Image Manipulation Dataset, http://www5.informatik.uni-erlangen.de, 2001.
[6] A. Popescu, H. Farid: *Exposing Digital Forgeries by Detecting Traces of Resampling*, SP 2005.
[7] J. He, Z. Lin, L. Wang, X. Tang: *Detecting Doctored JPEG Images Via DCT Coefficient Analysis*, ECCV 2006.
[8] M. Johnson, H. Farid: *Exposing Digital Forgeries through Chromatic Aberration*, M&S 2006.
[9] T. Gloe, K. Borowka, A. Winkler: *Efficient Estimation and Large-scale Evaluation of Lateral Chromatic Aberration for Digital Image Forensics*, SPIE Media Forensics and Security 2010.
[10] M. Johnson, H. Farid: *Exposing Digital Forgeries in Complex Lighting Environments*, TIFS 2007.
[11] C. Riess, E. Angelopoulou: *Scene Illumination as an Indicator for Image Manipulation*, IH 2010.
[12] R. Tan, K. Nishino, K. Ikeuchi: *Color Constancy through Inverse-Intensity Chromaticity Space*, JOSA 2004.