Should I Believe or Not? Adventures in Media Forensics

Information Access Division
National Institute of Standards and Technology, USA

ABSTRACT

Historically, the U.S. Government deployed and operated a variety of collection systems that provided imagery with assured integrity. In recent years, even relatively unskilled users can manipulate and distort the message of visual media. While many manipulations are benign, performed for fun or for artistic value, others are for adversarial purposes, such as propaganda or misinformation campaigns.

DARPA's Media Forensics (MediFor) program brings together world-class researchers to attempt to level the digital imagery playing field, which currently favors the manipulator, by developing technologies for the automated assessment of the integrity of an image or video and integrating these in an end-to-end media forensics platform.

(Adapted from: http://www.darpa.mil/program/media-forensics)

CONTACT

Jonathan Fiscus
P. Jonathon Phillips
Haiying Guan
Yooyoung Lee
Amy N. Yates
Andrew Delgado
Daniel Zhou
Multimodal Information Group,
Information Access Division
Information Technology Laboratory
National Institute of Standards and Technology
http://www.itl.nist.gov/iad/mig

Project

Motivations

Digital media manipulation software has progressed to the point where a cursory knowledge of the tools is sufficient to drastically change the information in the image, sometimes to the detriment of honest reporting. Current forensic tools used to detect or trace these manipulations lack robustness, scalability, and do not address all aspects of media authentication. MediFor aims to advance manipulation detection technologies through evaluation-centric research.

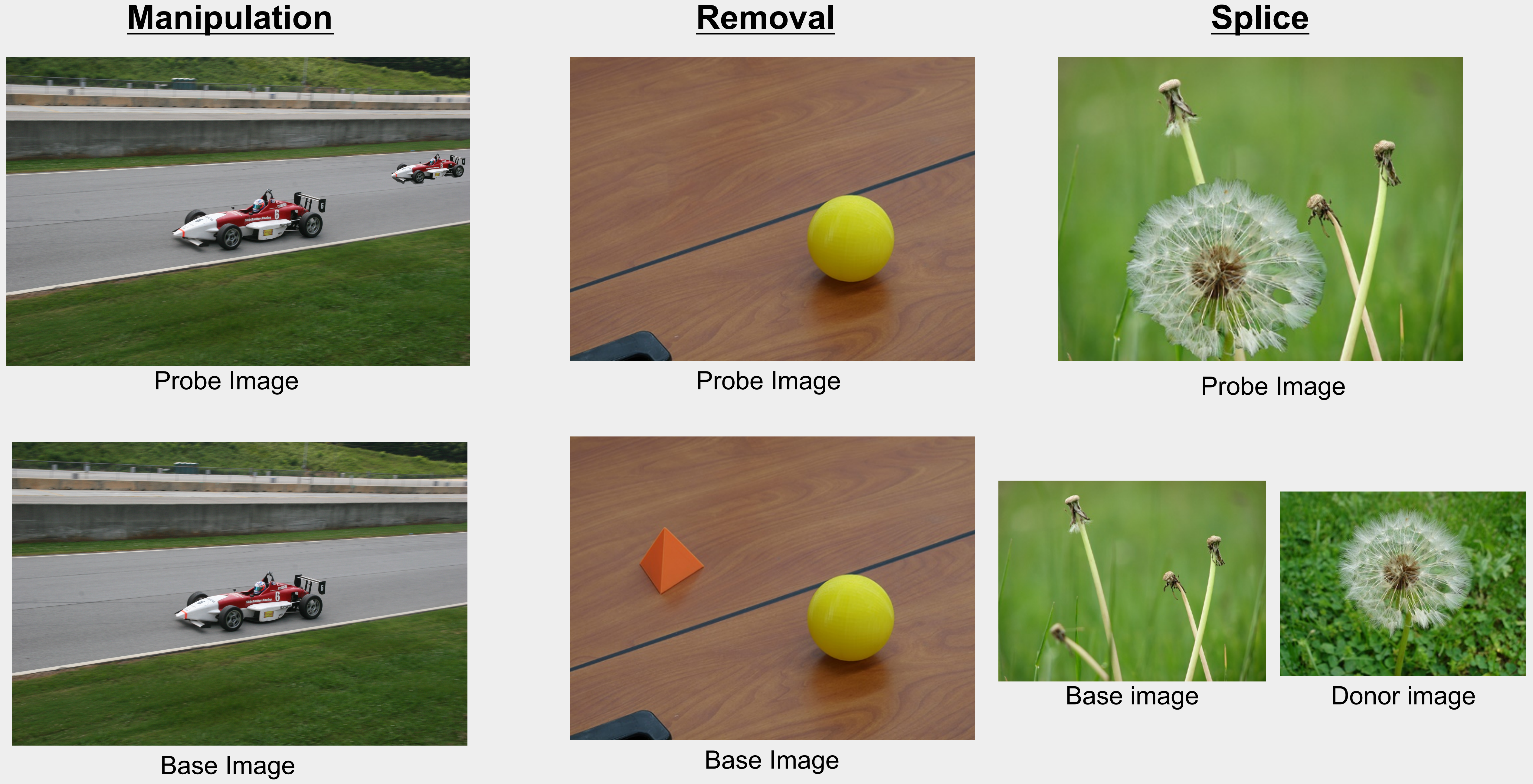
Approach

- Define a common lexicon of manipulation operations and descriptive metadata
- Design datasets to account for diverse manipulation types and sequences of manipulations
- Construct evaluation tasks to test both generic and specific manipulations by category, e.g. manipulation, removal, splice
- Design the evaluation infrastructure to account for the various manipulations

Impact

- Detect manipulations automatically and assist in forensic examination
- Provide detailed information about how these manipulations were performed
- Determine to what extent images are reliable

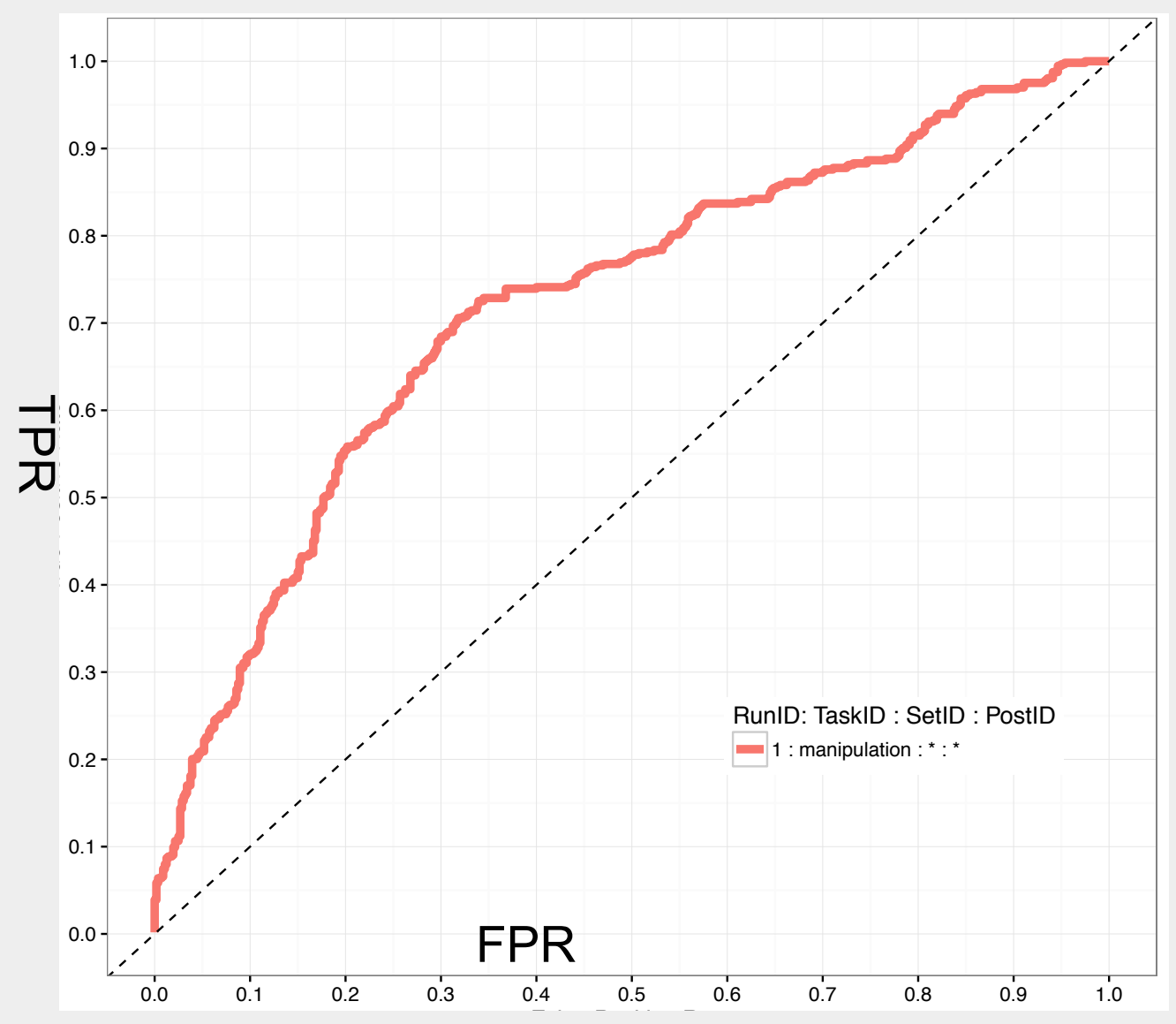
Manipulated Images



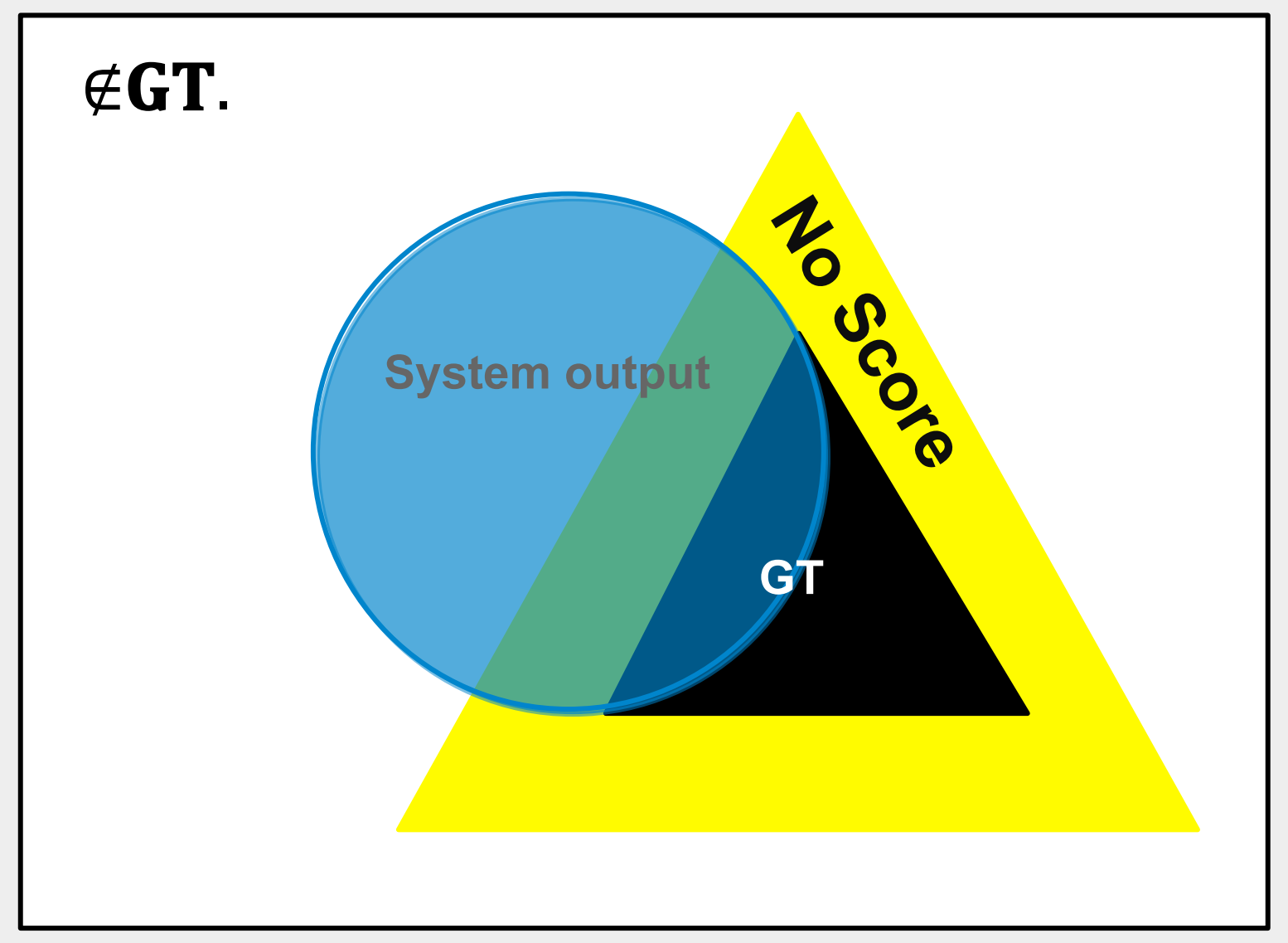
Sample images from the Nimble Challenge 2016 Dataset.

Metrics

ROC/AUC - Detection



Nimble Mask Metric (NMM)



System output mask

Probe reference mask

Results Analysis Question

- What general factors did the correctly identified images have that the incorrectly identified images did not?
- Which factors enabled the algorithm to make this decision?

Next Steps

- Evaluate algorithms on the dataset
  - ○ Detection
  - ○ Region of manipulation (mask)
  - ○ Provenance
- Extend to video