CAREER: Scaling Forensic Algorithms for Big Data and Adversarial Environments

Challenge:

- Images and videos can be easily falsified

- New, scalable algorithms must be developed to:
  - Identify complex image/ video forgeries
  - Efficiently examine large volumes of data
  - Respond to adversarial information attackers

Solution:

- Improve efficiency through theoretical analysis

- Develop theoretical framework model complex editing traces

- Study attacker's anti-forensic capabilities

Matthew C. Stamm (PI), Drexel University

mcstamm@coe.drexel.edu

Award Number: 1553610

Program Manager: Deborah Shands

Image Forgery

⬇

Forensic Feature Extraction

⬇

Detection Algorithm

⬇

Falsified Regions Identified

Scientific Impact:

- New theoretical models to guide future research

- Algorithmic building blocks to construct sophisticated forgery detection algorithms

- Characterization of forger's capabilities and optimal response

Broader Impact:

- Help bring trust to images and videos

- Software library of forensic algorithms

- Benchmarking data sets

- Outreach to general public

- Establish multimedia forensics challenge to foster research activity