



MERIT
2007 FAIR

Digital Image Detective: Using Forensic Analysis to Identify Image Source

Christine McKay

Advised By: Ashwin Swaminathan, Hongmei Gou, Dr. Min Wu

**MERIT Program, Electrical and Computer Engineering Department
University of Maryland, College Park**



Multimedia Forensics

Where Sherlock Holmes meets Signal Processing

❑ Image Source Forensics

- How was the image created? Camera, scanner, cell phone camera or via computer graphics
- What **type** of device captured the image?

❑ Device Model Identification

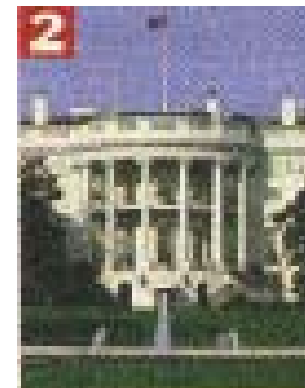
- What **model** of camera, cell phone camera, or scanner captured the image?

❑ Forgery detection

- Is the image **tampered**? or manipulated after capture?



Image Tampering

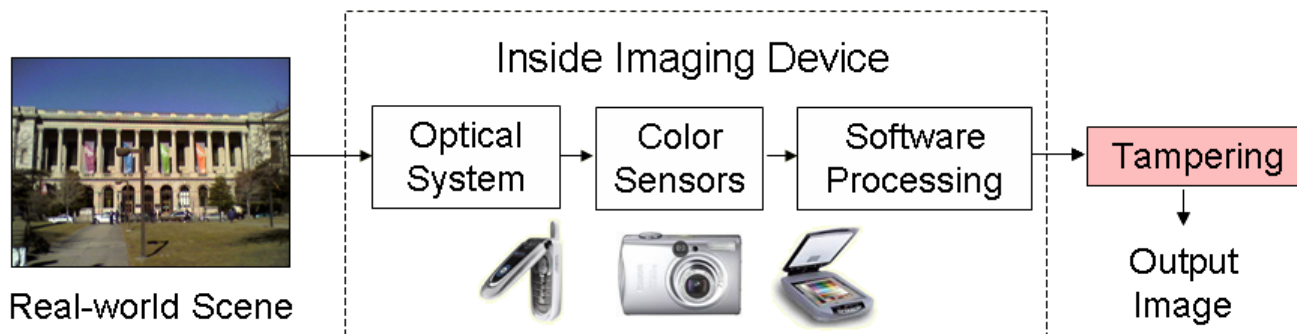


Source: Federal Computer Week, 1998



Non-Intrusive Forensics

- ❑ Identify **distinguishing features** of an image acquisition device using its **output data** alone
- ❑ Image acquisition process

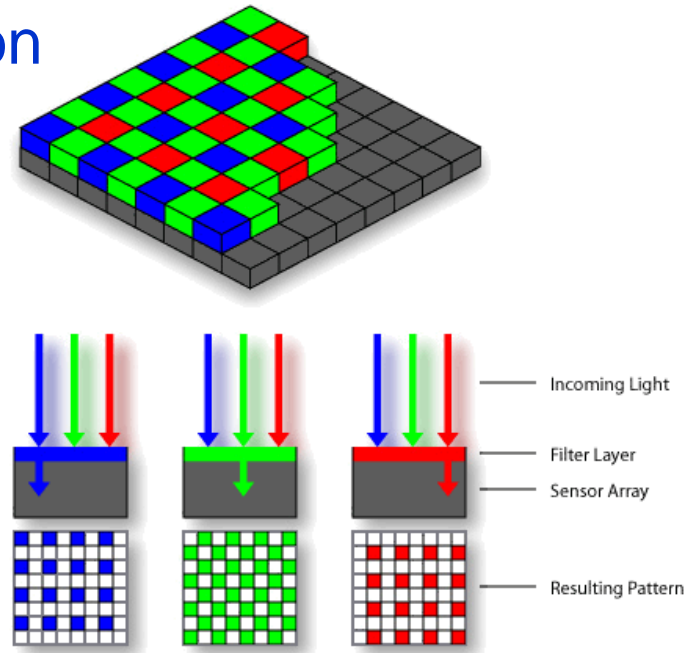


- ❑ Find and exploit differences in optical system, sensors, and software among devices using sample images

Features for Forensic Analysis

□ Color Filter Arrays and Interpolation

- Scanners detect all three colors at each pixel
- Cameras only detect one color at each pixel
 - Remaining two colors estimated using **interpolation** algorithms

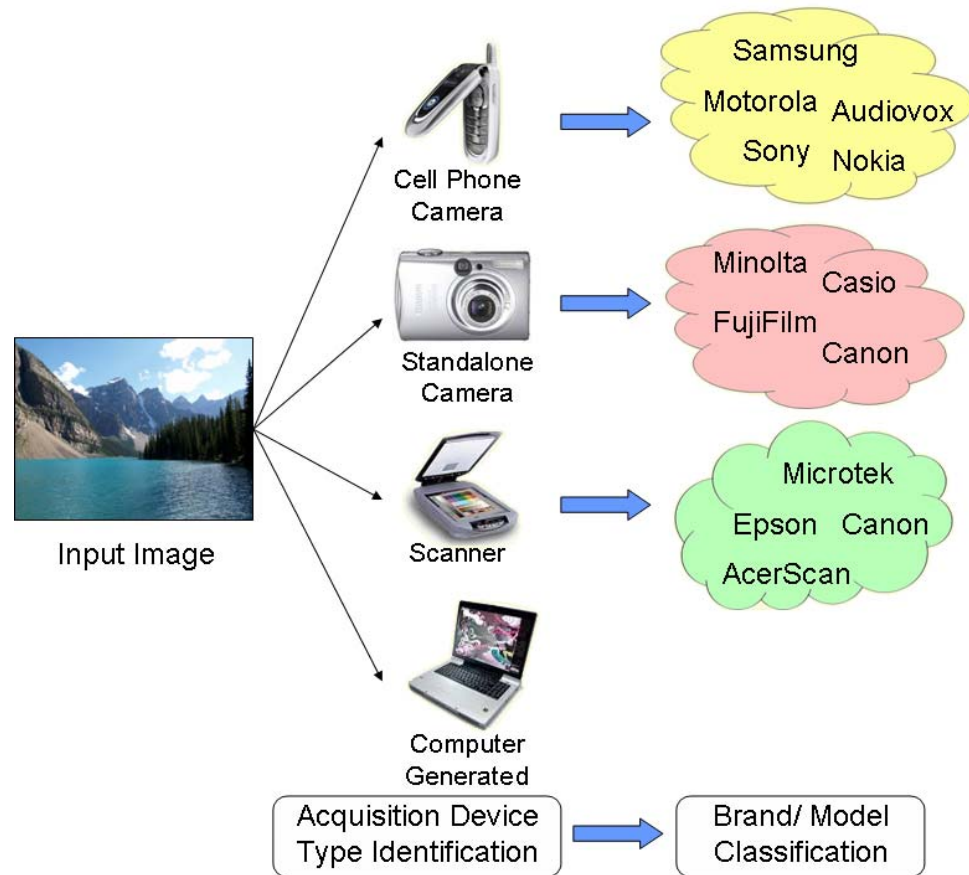


□ Noise

- Inherent in any electronic device
- Measure variations in pixel values under no light or constant light

Forensic Methodology and Roadmap

- Estimate **interpolation coefficients** and **noise features** for each device using random sample images
- Use these data to create a **model** to identify the source of an unknown image



Demo

Image Device Identification Demo

Select an Image

Device: Standalone Camera

Image (1)

- Choose a Device
- Cell Phone Camera
- Standalone Camera
- Scanner
- Computer Generated

Device Identification

Identify

Standalone Camera

Correct!

Test Camera Identification

