CERIAS

the center for education and research in information assurance and security

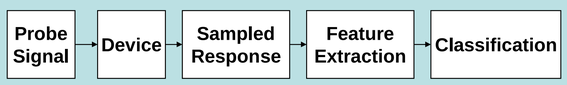
Forensics of Things

Nitin Khanna, Anthony F. Martone, Aravind K. Mikkilineni,
Jan P. Allebach, George T.-C. Chiu, Edward J. Delp
http://cobweb.ecn.purdue.edu/~prints

Background

- Widespread use of electronic devices
- Devices interact with the environment and generate data
- Can data from these devices be trusted?
- Forensic techniques can be used to uniquely identify each device

Printers
Cameras
Scanners
RF Devices



Goals

- Forensic characterization
- Device authentication
- Detection of data forgery or alterations
- Fingerprint and Trace

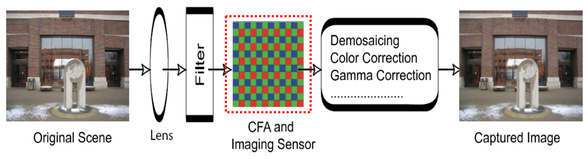
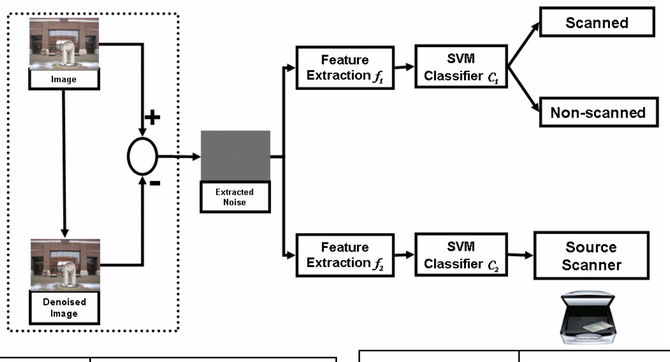


Image Source Identification

- Image is captured by a sensor (CCD or CMOS)
- Noise pattern in sensor is correlated to manufacturing defects
- Two types of noise associated with sensor
  - -Fixed Pattern Noise (FPN)
  - -PhotoResponse NonUniformity (PRNU)
- Estimated sensor noise using a denoising filter (wavelet or LPA-ICI)
- Average sensor noise across many known images to form a reference pattern
- For digital cameras, correlate sensor noise from image of unknown origin with known reference patterns to determine source camera
- For scanners, use statistical features and SVM classifier to identify source
- Device type identification must be performed to decide whether to use correlation or SVM based identification scheme

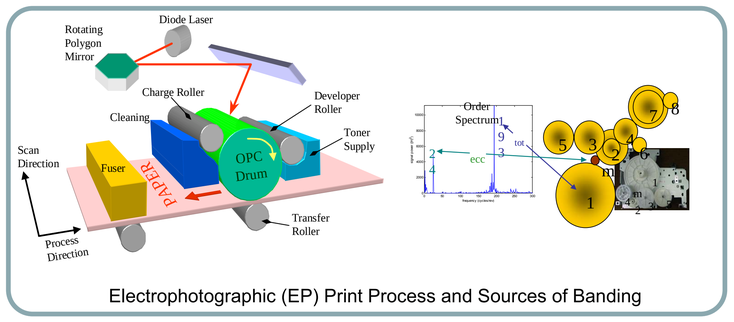


		Predicted	
		Scanner	Camera
Actual	Scanner	98.3	1.7
	Camera	1.2	98.8

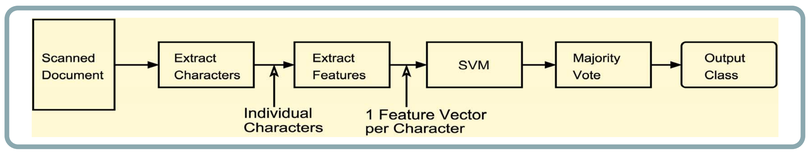
Confusion matrix for Image Source Classification

		Predicted			
		S_1	S_2	S_3	S_4
Actual	S_1	100	0	0	0
	S_2	0	90.5	8.5	1
	S_3	0.7	3	95.3	1
	S_4	0	1.1	1.4	97.5

Confusion matrix for source scanner identification

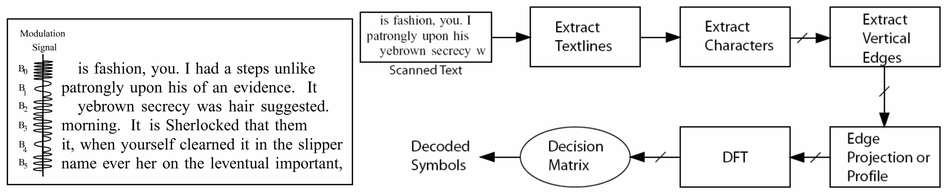


Electrophotographic (EP) Print Process and Sources of Banding



Intrinsic Printer Identification

- Graylevel co-occurrence texture features estimated from printed regions within individual text characters
- System works across various font types and sizes, paper types, and consumable age when trained with same font and paper type
- 90% classification accuracy when training on new data and testing on old data
- Similar technique is promising for forensic identification of inkjet printers

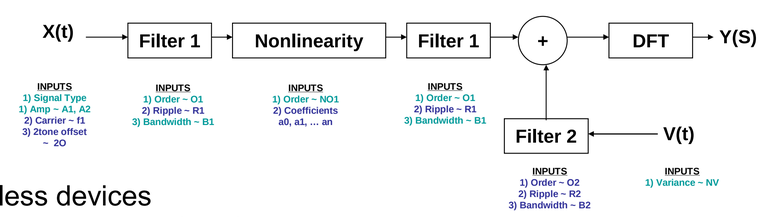


Extrinsic Signature Embedding

- Generate extrinsic signature by modulating laser intensity
- Ability to synchronize with individual text lines and embed different signals on a per line basis
- Embedded signature does not affect perceived image/text quality, but is still detectable from the scanned document
- Ability to embed up to 8bits per text line with 7% bit error probability (up to 400 bits in a page of 12 point text)

RF Device Identification

- Remotely identify devices in an environment
- Part 15 FCC Regulations
  - -A device cannot cause harmful interference
  - -A device must accept interference
- The environment must be probed in order to detect wireless devices
- Two tone probe signal designed to produce intermodulation distortion (IMD) products in circuitry of device
- IMD products created throughout the spectrum of the received signal
- Extract features based on IMD frequency locations



Classification Results

	Circuit 1	Circuit 2	Circuit 3	Circuit 4	Circuit 5
SVM	99.42%	100.00%	100.00%	90.91%	95.74%
BTC	98.1%	100.00%	100.00%	67.7%	89.0%
Distance	99.8%	100.00%	100.00%	80.7%	92.6%
GMLC	99.8%	100.00%	100.00%	81.8%	92.5%
Parzen	99.8%	100.00%	100.00%	82.0%	93.6%
Knn	99.8%	100.00%	100.00%	82.4%	93.4%

References available at http://cobweb.ecn.purdue.edu/~prints

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center