Multimedia Security: A Viewpoint From A Walking Wounded

Edward J. Delp

Video and Image Processing Laboratory(*VIPER*)
School of Electrical and Computer Engineering
School of Biomedical Engineering
Purdue University
West Lafayette, Indiana

email: ace@ecn.purdue.edu

http://www.ece.purdue.edu/~ace

Multimedia Security: A Viewpoint From A Walking Wounded

Edward J. Delp

Academy of Finland Distinguished Professor Program (FiDiPro)
Tampere University of Technology
Tampere International Center for Signal Processing (TICSP)
Tampere, Finland

delp@cs.tut.fi
http://www.cs.tut.fi/~delp

Video and Image Processing Laboratory Research Projects

- Video Compression
  - Low complexity coding
  - Scalable Coding
  - Wyner-Ziv Approaches
  - Texture Based Methods
- Error Concealment, Resilience, and Post-Processing
- Video Databases
  - Indexing user generated content
  - Location awareness
- Multimedia Security and Forensics

Video and Image Processing Laboratory Research Projects

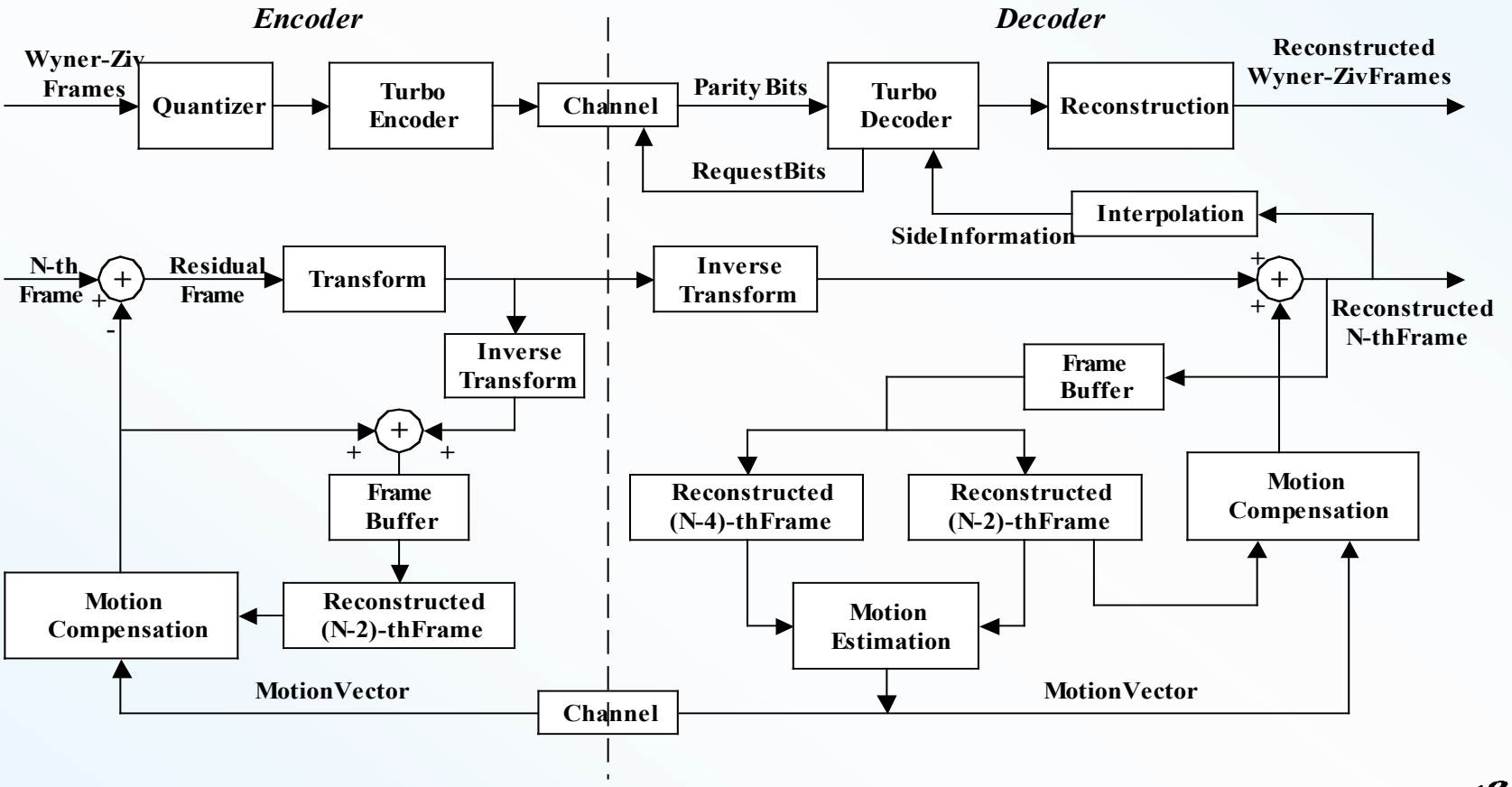
- Video Tracking and Surveillance
- Medical Imaging
  - Microscope image analysis
- Mobile Applications
  - Image Guided Navigation - location awareness
  - Language Translation
  - Food and Dietary Assessment
- Content Adaptation
- Digital Cinema
- Social Networking

Image and Video Processing at Purdue

Purdue has a rich history 75 year history in image and video processing

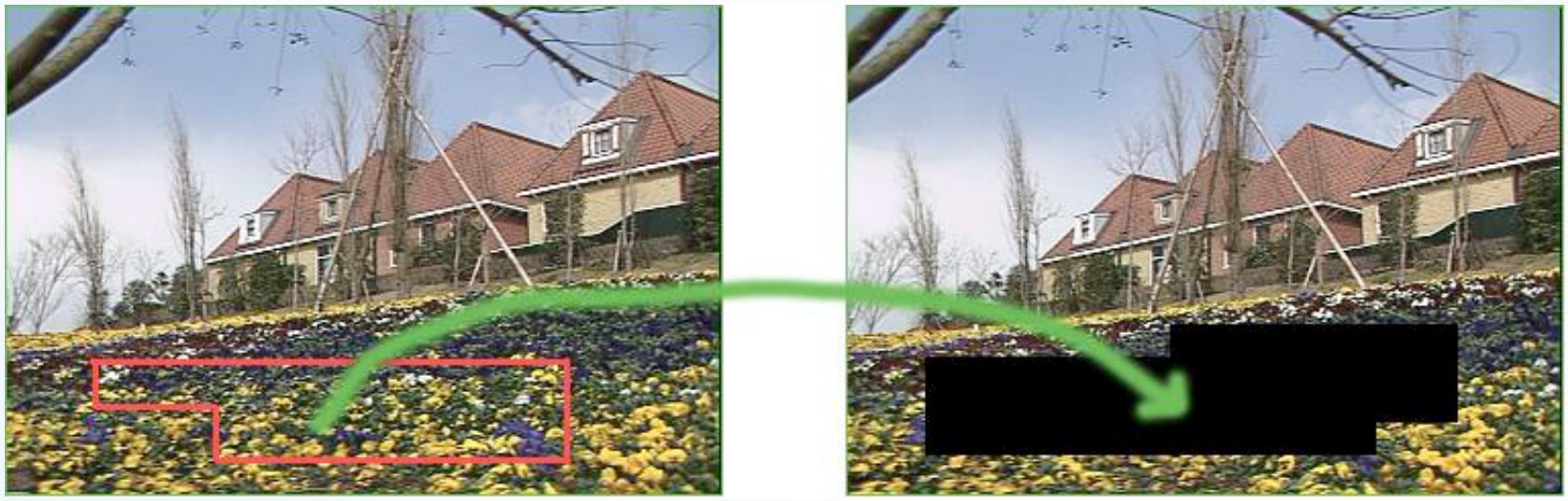
First Ph.D. in digital image processing in 1959

Low Complexity Video Compression System

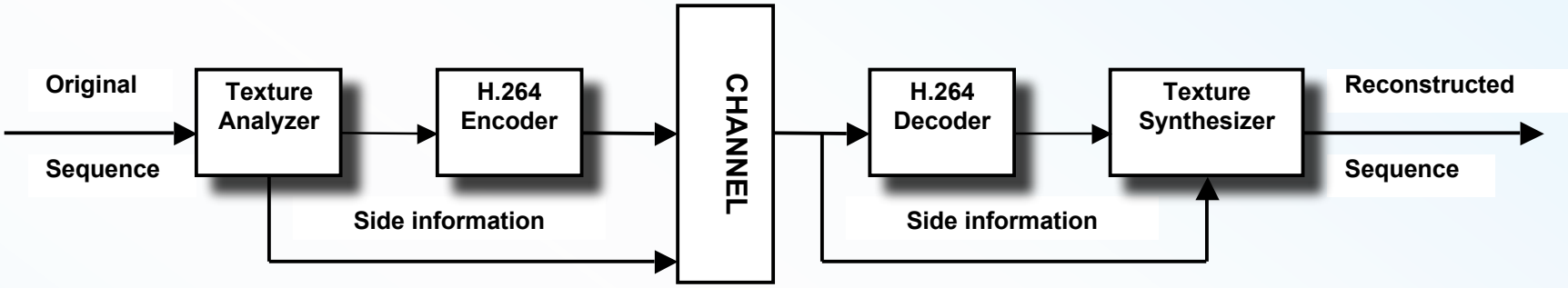


Segmentation Based Compression: Basic Concept

"Reference" Frame **Current Frame**



System Overview



- **Texture Analyzer**
  - **Identifies homogenous regions in a frame and labels the regions as textures**
  - **Use global motion models to ensure temporal consistency**
- **Encoder and Decoder: Conventionally codes the sequence with synthesizable regions labeled as skipped macroblocks**
- **Texture Synthesizer: Inserts synthesizable parts using the side information**

Flowergarden Frame 58

(a)

(b)

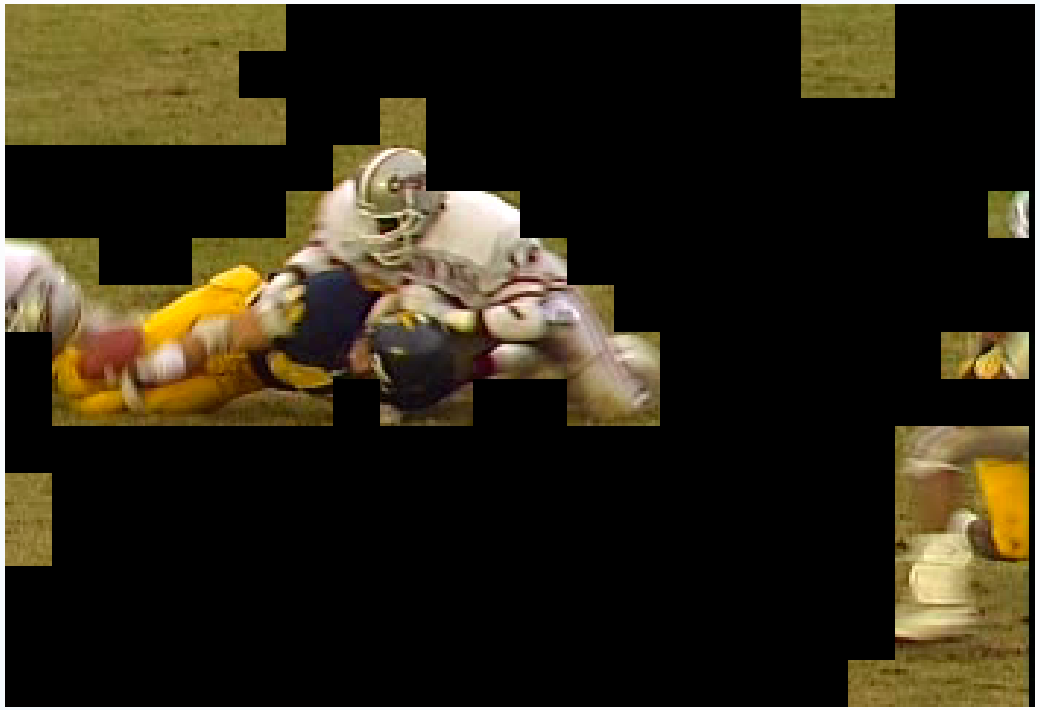
(c)

(a) original frame

(b) reconstructed frame

(c) synthesizable texture mask

Texture Analysis



Football Sequence

Original

Reconstructed

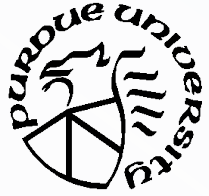
Mobile Video Content

Personal Content or Unstructured Video

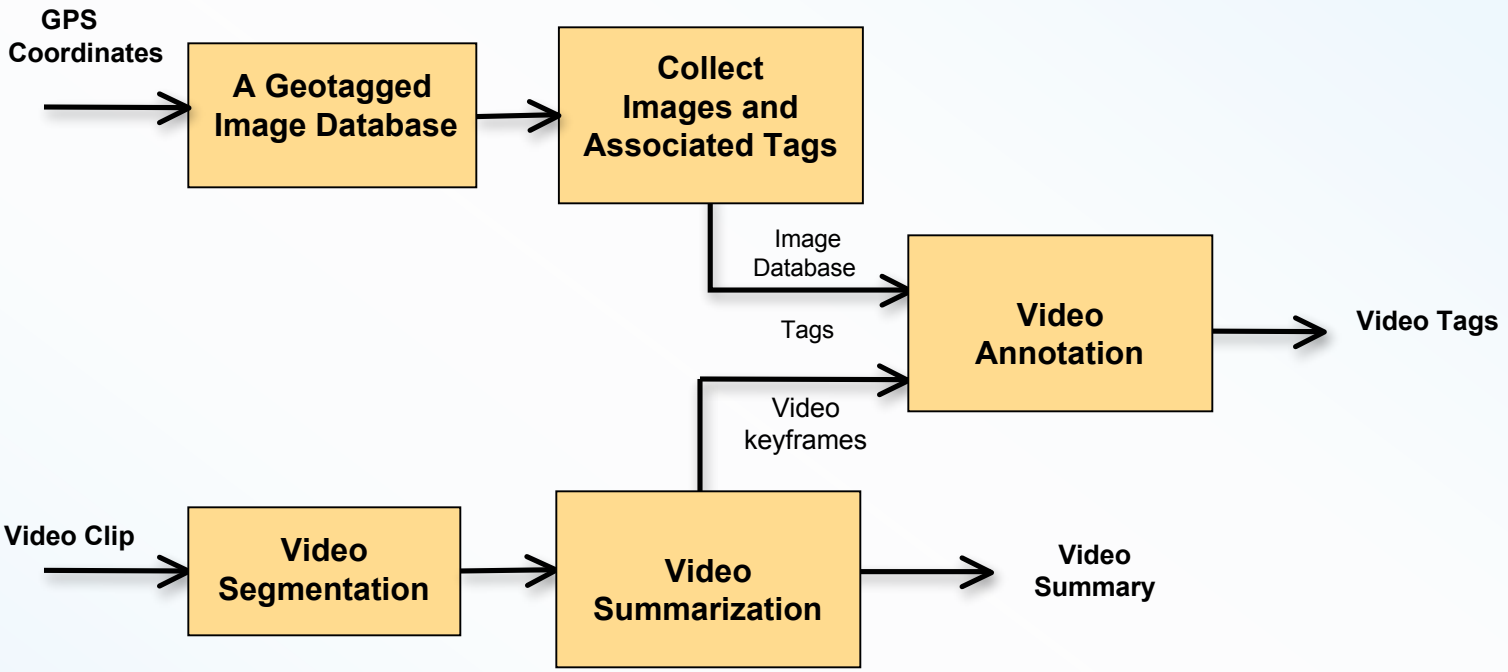
- captured by the user using the camera on the device

Commercial Content or Structured Video

- (e.g. news, sports, and music videos) streamed or downloaded into the device

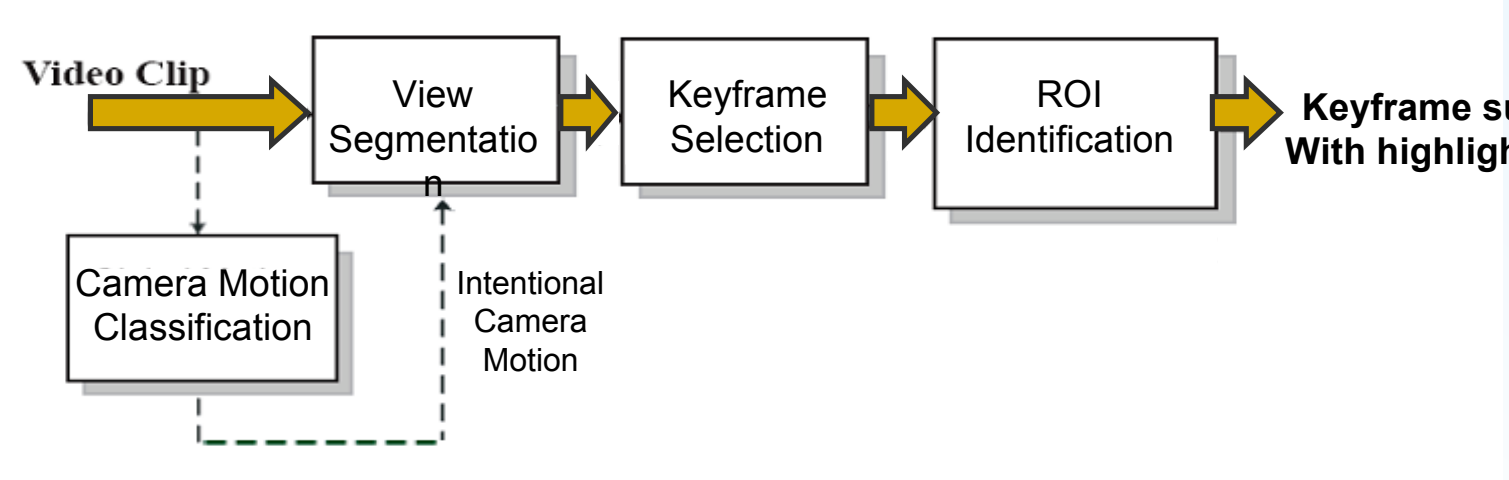


System Overview

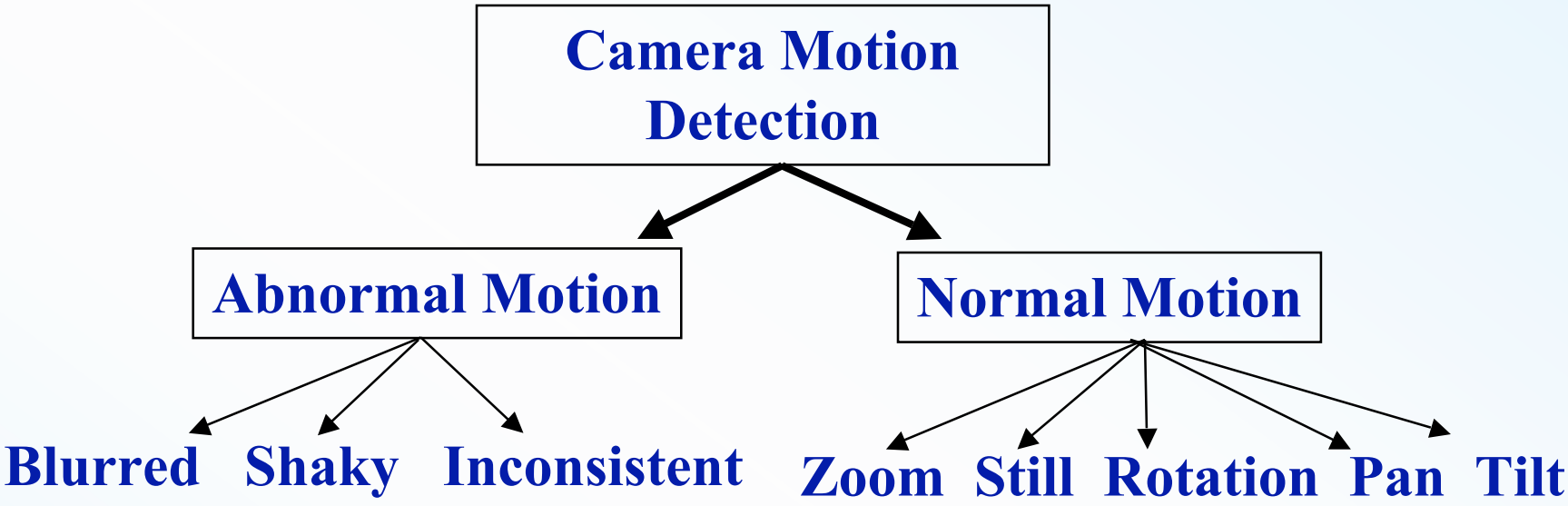


- **Goal - use camera motion and GPS metadata to find annotated pictures with the same coordinates in an image database and use them to automatically annotate (tag) user generated video**

Motion-Based Video Summarization



- **User Generated Video (UGV) often has a rich camera motion structure that generated by the camera person**
- **We use this structure in different steps of the analysis**
- **Camera motion in UGVs contain both intentional motion (pan, tilt and zoom) and unintentional (blurry and shaky) motion**



- ***Blurred*** segments are caused by fast camera motion
- ***Shaky*** segments are caused by frequent change of direction
- ***Inconsistent*** segments are caused by uneven acceleration of camera

Video Labeled By Type

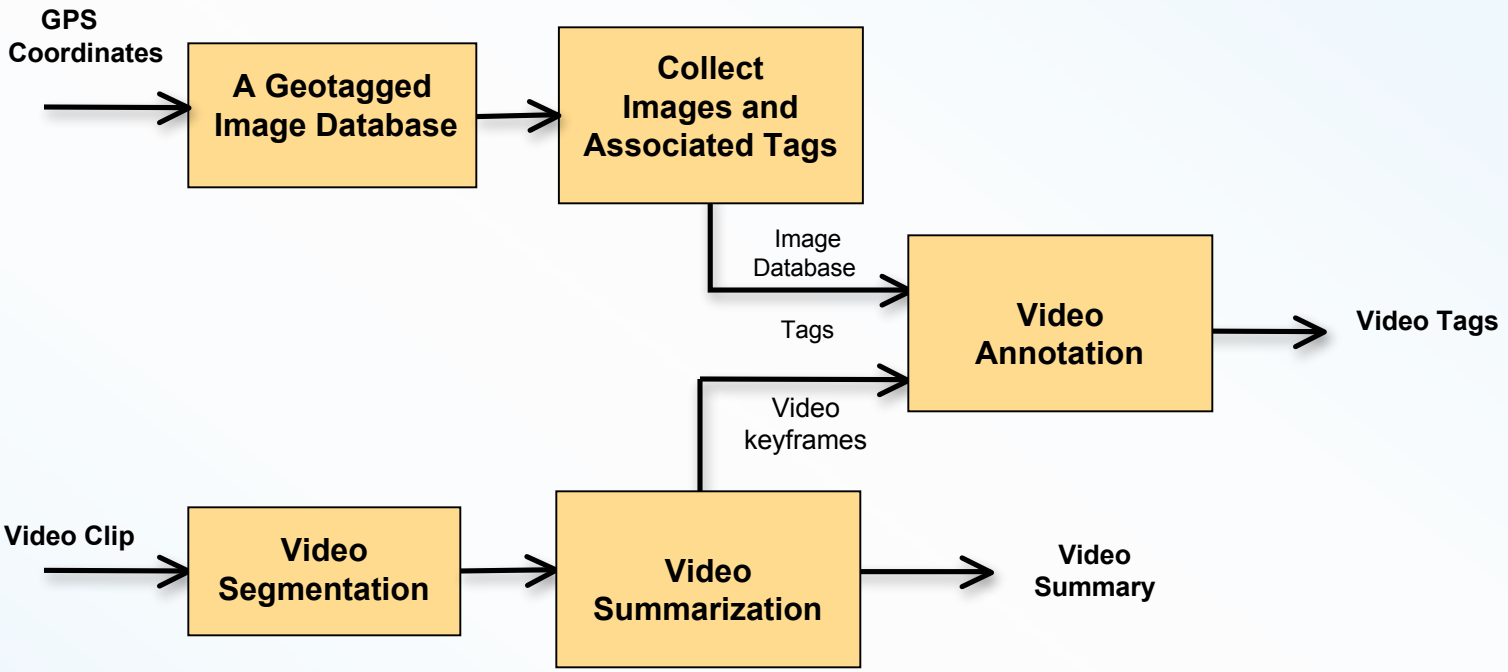
Color Contrast Saliency Maps

ROIs






System Overview



- **Goal - use camera motion and GPS metadata to find annotated pictures with the same coordinates in an image database and use them to automatically annotate (tag) user generated video**

Example-A Geotagged Image Database

Examples

Query Keyframe

The 8 most similar images in the dataset

g3

Rosetta Phone

System Overview

Image Acquisition

Segment

OCR

TTS

Display

رحیم یار خان

Transliteration: Rahim Yaar Khan
Translation: Rahim Yaar Khan
Context: Town Name

Audio Output

-Spoken Text in Original Language
-Spoken English Translation of Text

Rosetta Phone System

- **Natural scene image acquisition**
- **Text segmentation**
- **Optical character recognition**
- **Text interpretation**
- **Audio output**

Location-Aware Image Database (*LAID)*

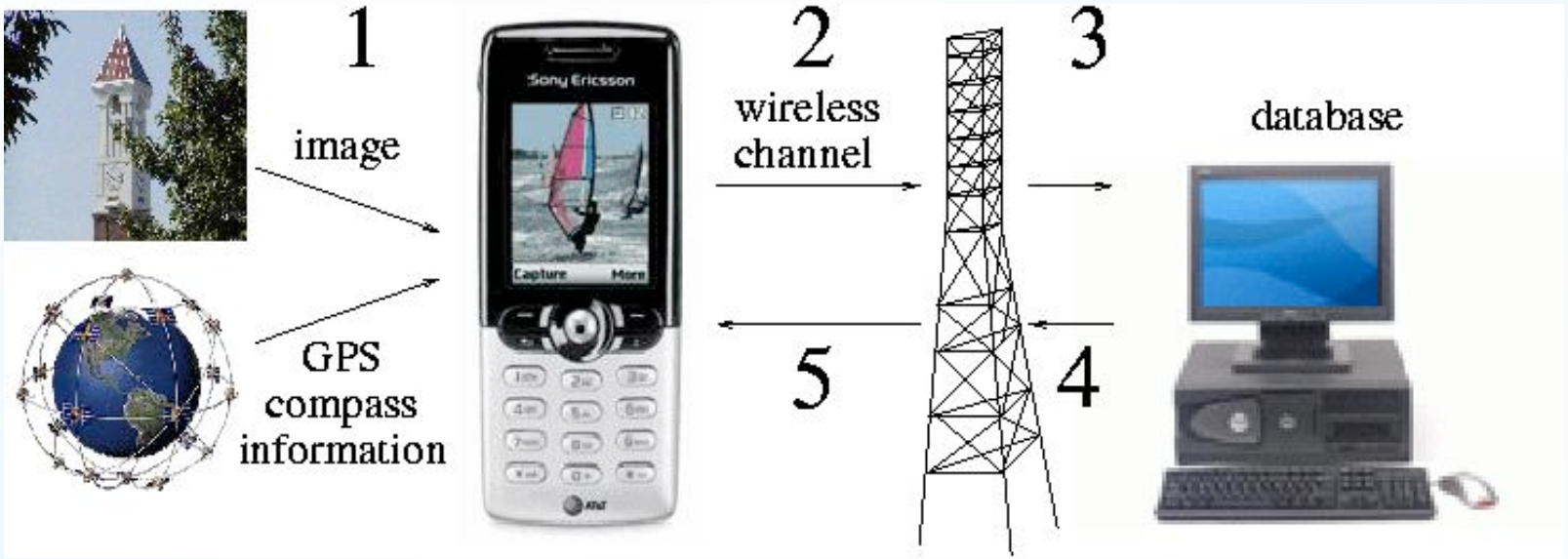


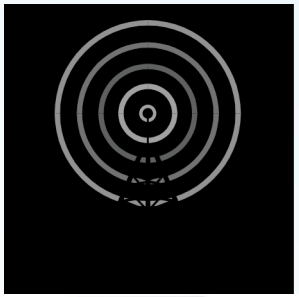
Image-Assisted Localization

+ Navigation

GPS and compass information

image

query through wireless network



thumbnail + description

information about the objects in the image

direction

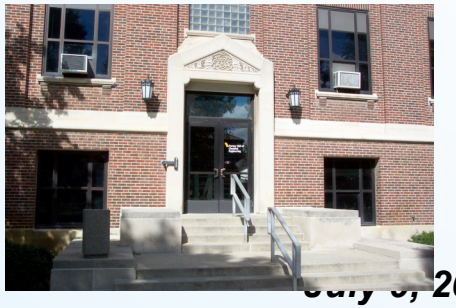
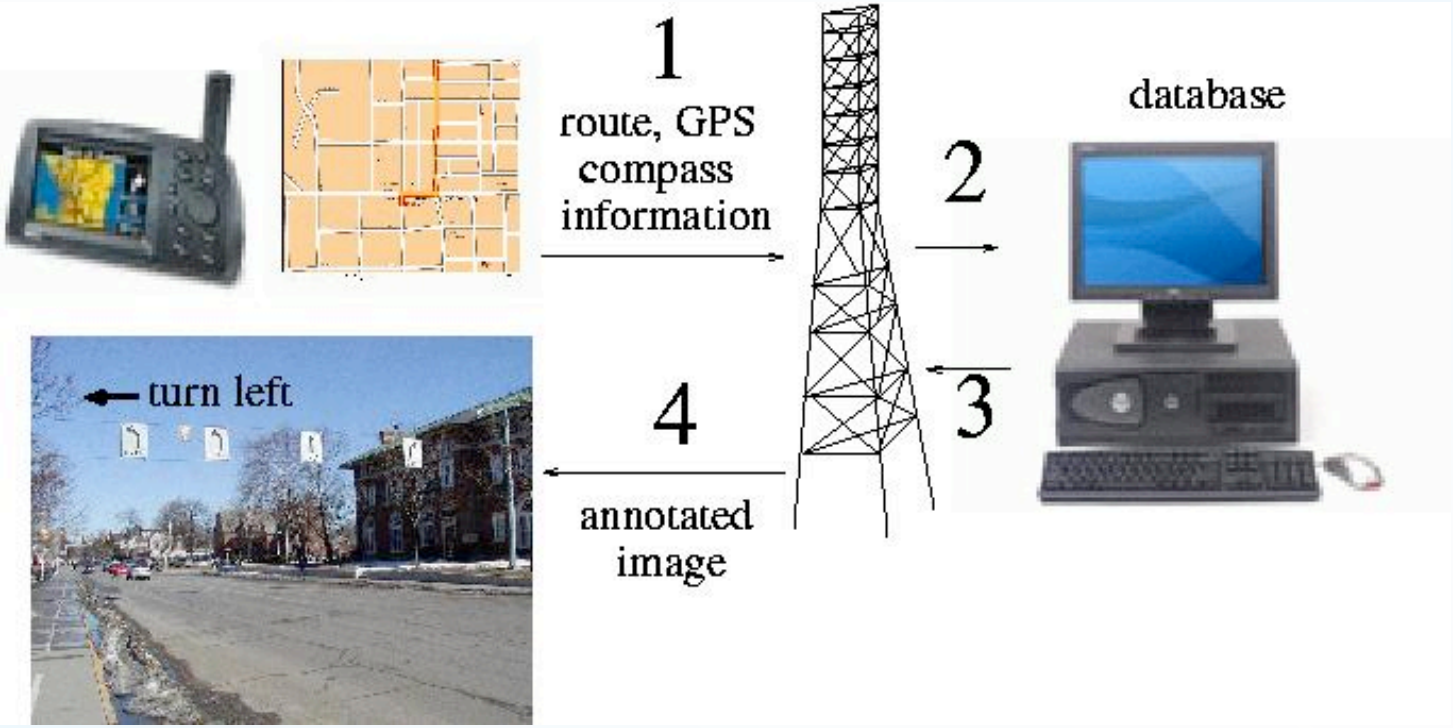
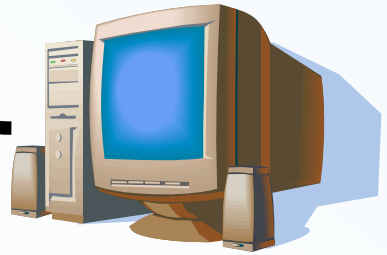


Image-Enhanced Navigation
(IEN)



Building and Using the Database



www.tadaproject.org

Extract

toast

Pork Rib

steak

Before Meal

Plate Waste

Food intake comparison

TADA System Overview

Client

Image + Metadata

1

4

Server

2

- Food Type (Label)
- Labeled Segmented Images (Area Estimates)

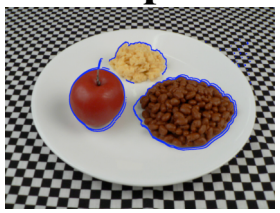
3

Volume Estimation

Output

- Labeled Images With Food Type (e.g. Apple, Beans, Eggs)
- Volume

+



5

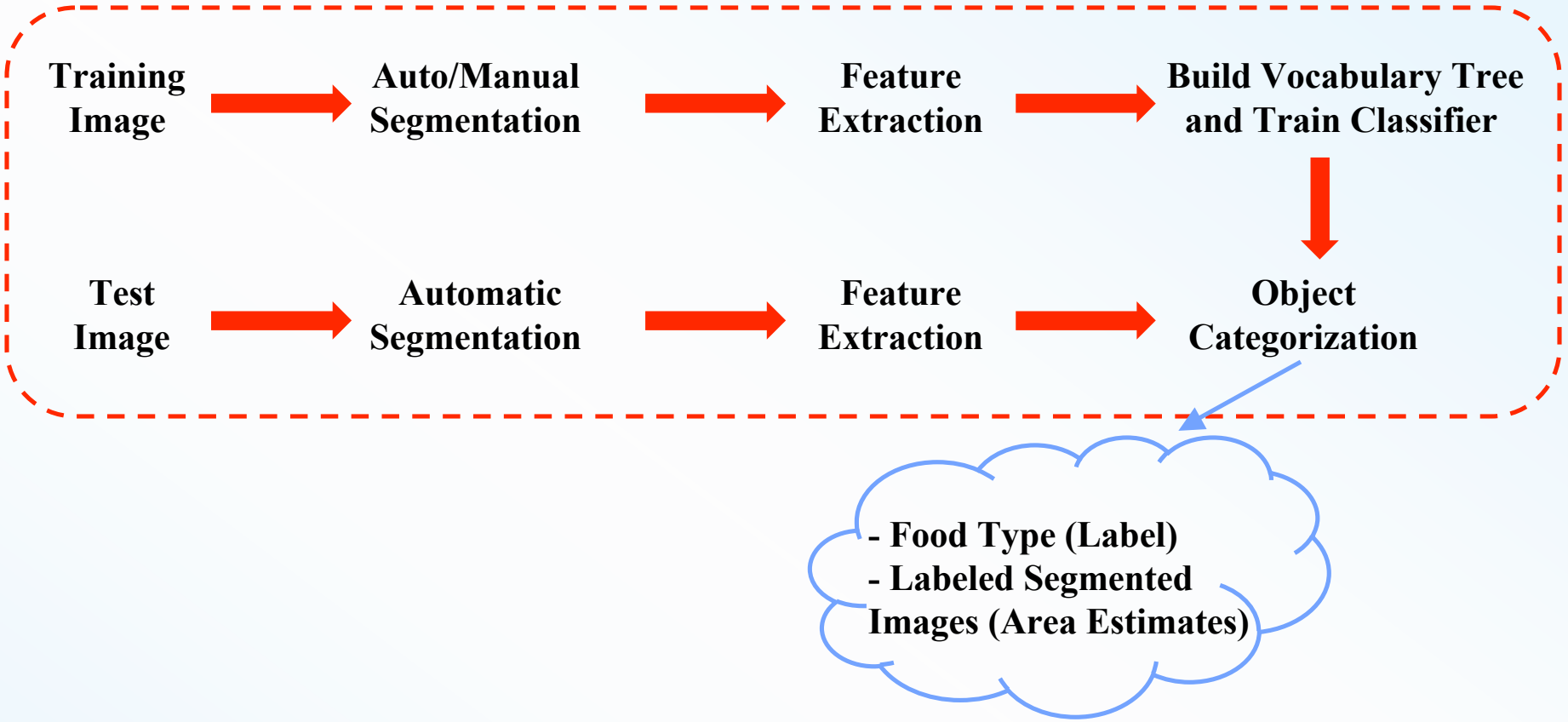
User Confirmation and Adjustment

6

- FNDDS Indexing
- Nutrient Information

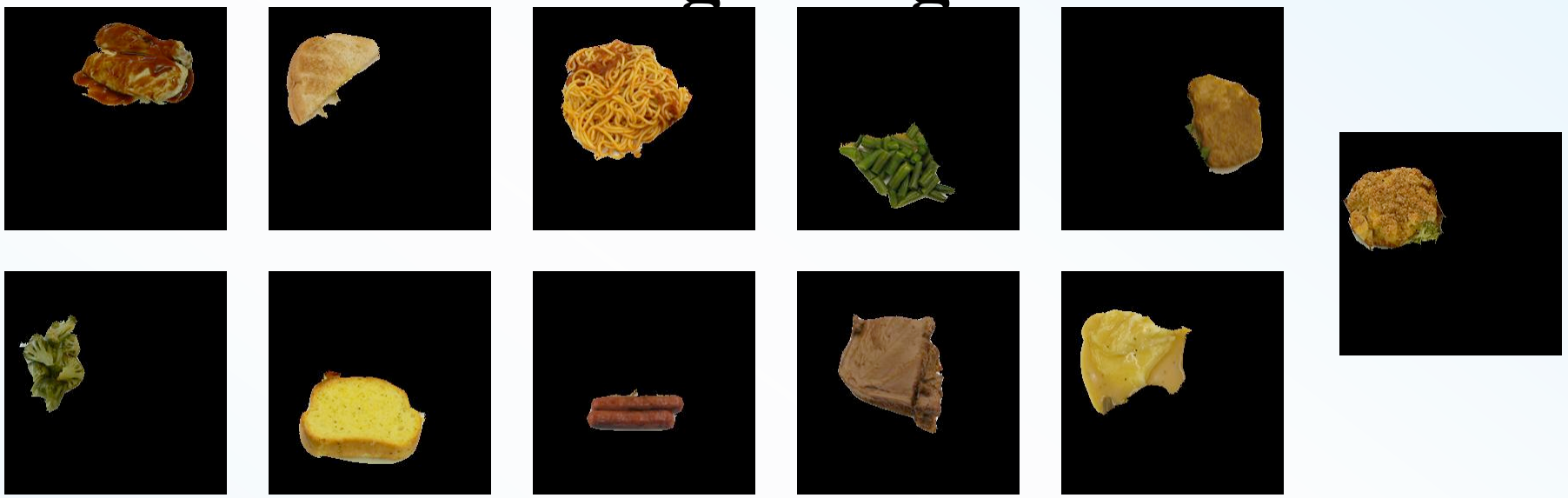
7

Research Community



- **Training images – categorized database containing single object images**
- **Segmentation – Normalized Cut, Connected Components**
- **Features – color, texture, SIFT**
- **Categorization – Bag of Features object recognition**

Building Categories

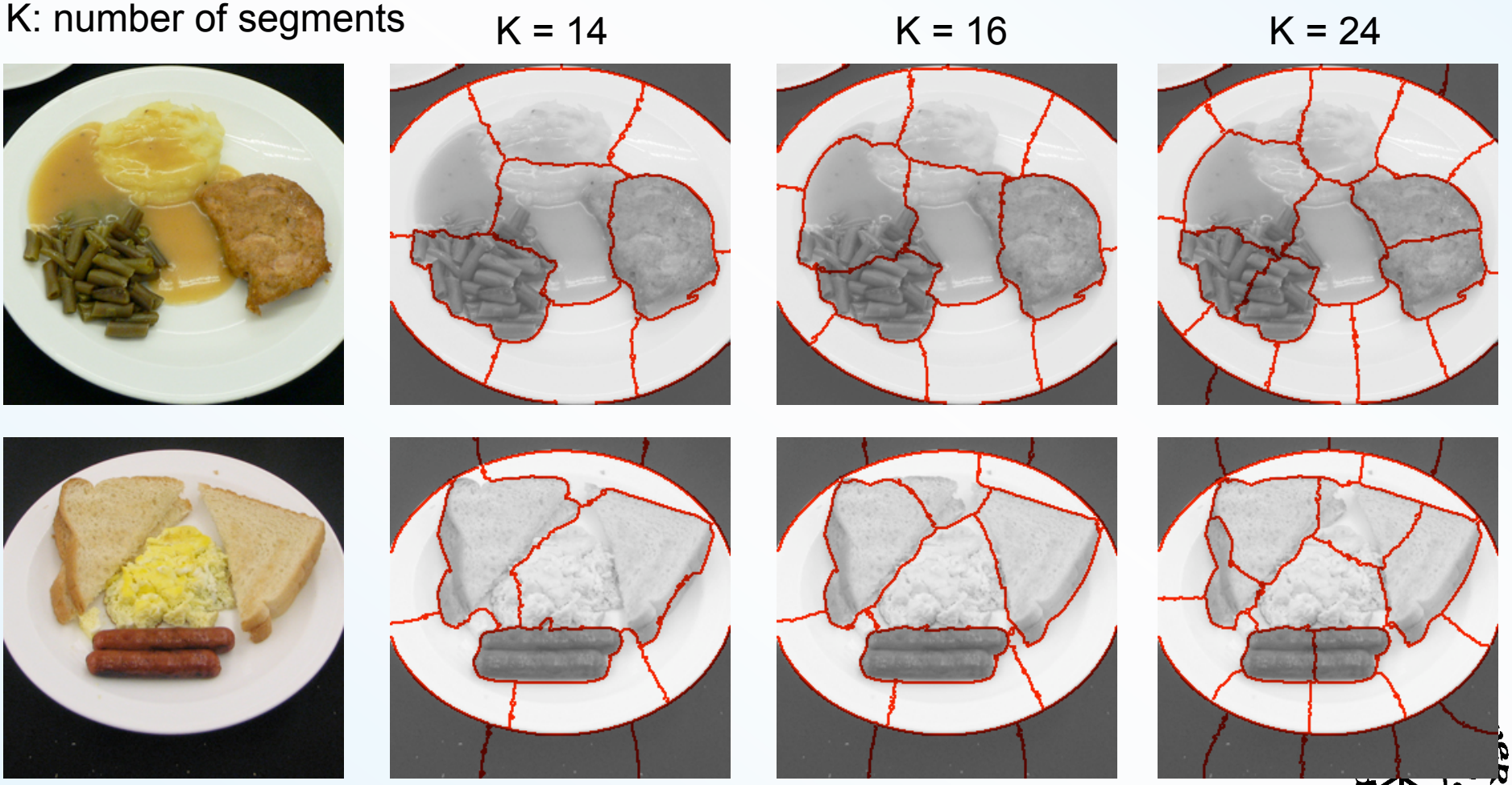


- **Normalized Cut to extract segments from the image**
- **Brightness as cue, image size 256x256**
- **Each category contains different images of the item**

Issue with Normalized Cut

- **Difficulty with some images**

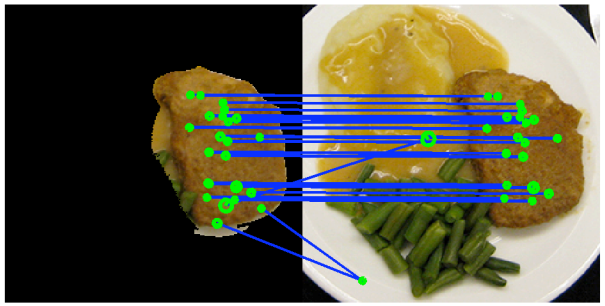
K: number of segments



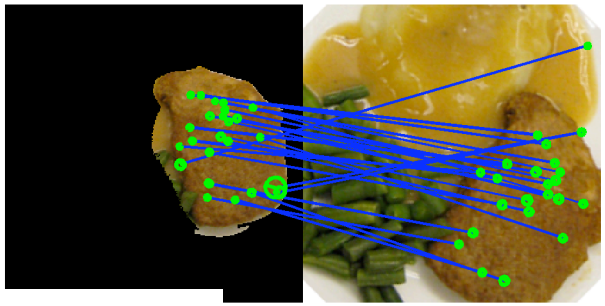
Extract Feature

- **SIFT descriptor for matching**

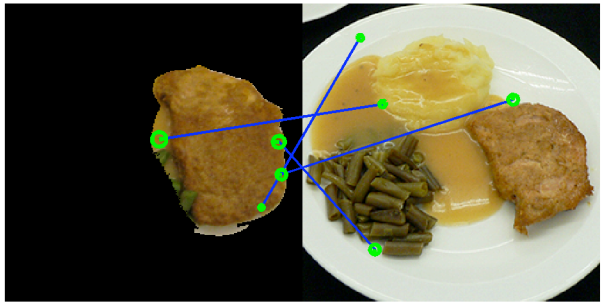
Same item



Same item, image scaled and rotated



Different item of same category



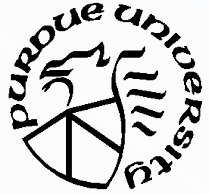
Multimedia Security: Yuck!

Overview

- **"Securing" multimedia content is a hard and undefined problem**
- **Problem started with "cute" applications and evolved into the "monster" of content protection**
  - **World-wide losses from piracy is estimated at more than $30 billion**

Content Protection Objectives

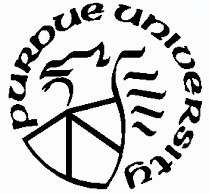
- **"Keeping Honest People Honest!"**
- **Prevent unauthorized access and use of digital content**
- **Prevent creation of illegal copies**
- **Audit usage of digital content**
- **Tamper detection, forgery detection, authentication**
- **Maintain rights and privileges expected by users, including "First Sale" and "Fair Use"**
- **Maintain user privacy**



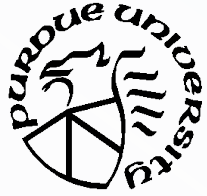
What Do Content Owners Want?

- **Access Control**
- **Copy Control** $\Rightarrow$ Playback Control, Record Control, Generation Control

- **Auditing (fingerprinting)**
  - **Who did what and when?**



Media protected		Secure delivery of content	Device authentication	Association of digital rights	Licensed technology	System renewability
Prerecorded media	Video on DVD-ROM	encryption	Mutual between DVD drive and PC	metadata	CSS [8]	Device revocation
	Audio on DVD-ROM	encryption	Mutual between DVD drive and PC	metadata	CPPM [36]	Device revocation
		watermarking	n/a	watermark	4C/Verance Watermark [37]	n/a
	Video or audio on DVD-R/RW/RAM	encryption	Mutual between DVD drive and PC	metadata	CPRM [38]	Device revocation
	Video on digital tape	encryption	n/a	metadata	High Definition Copy Protection [39]	Device revocation
Digital interface	IEEE 1394	encryption	Mutual between source and sink	metadata	DTCP [40]	Device revocation
	Digital Visual Interface (DVI)	encryption	Mutual between source and sink	metadata	HDCP [41]	Device revocation
	NRSS interface	encryption	Mutual between host and removable security device	metadata	Open standards [42]–[44]	Service revocation
Broadcasting	Satellite	encryption	None	metadata	Conditional access system [45], [46]	Smartcard revocation
	Terrestrial	encryption	None	metadata	Conditional access system [46]	Smartcard revocation
Cable transmission		encryption	None	metadata	Conditional access system [47]	Smartcard revocation
Internet	Unicast	encryption	Receiver	metadata	DRM [48], [49]	Software update
	Multicast (A few watermarking schemes have been proposed for multicast data [50])	encryption	Sender and receiver (depends on the authentication type)	metadata	Group key management [50]	tbd



What Do Users Want?

- **Leave me alone!**
- **Make it easy to use and interoperate with other things I own!!**
- **Content Protection is not a "feature"**

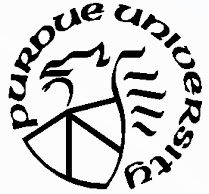
- **Time-shifting (Tivo)**
- **Format-shifting (iPod)**
- **Location Shifting (Slingbox)**
- **Single copy (back ups?)**

Re-distribute - Copies to your 10,000 closest friends?

How to Fix the Problem?

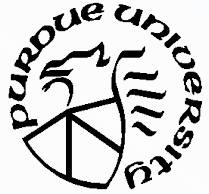
- **Technology - crypto, watermarking?**
- **Legal - DMCA?**
- **Moral Issues - is stealing good for you?**
- **Education - should stealing be good for?**

Should "bits" be free?

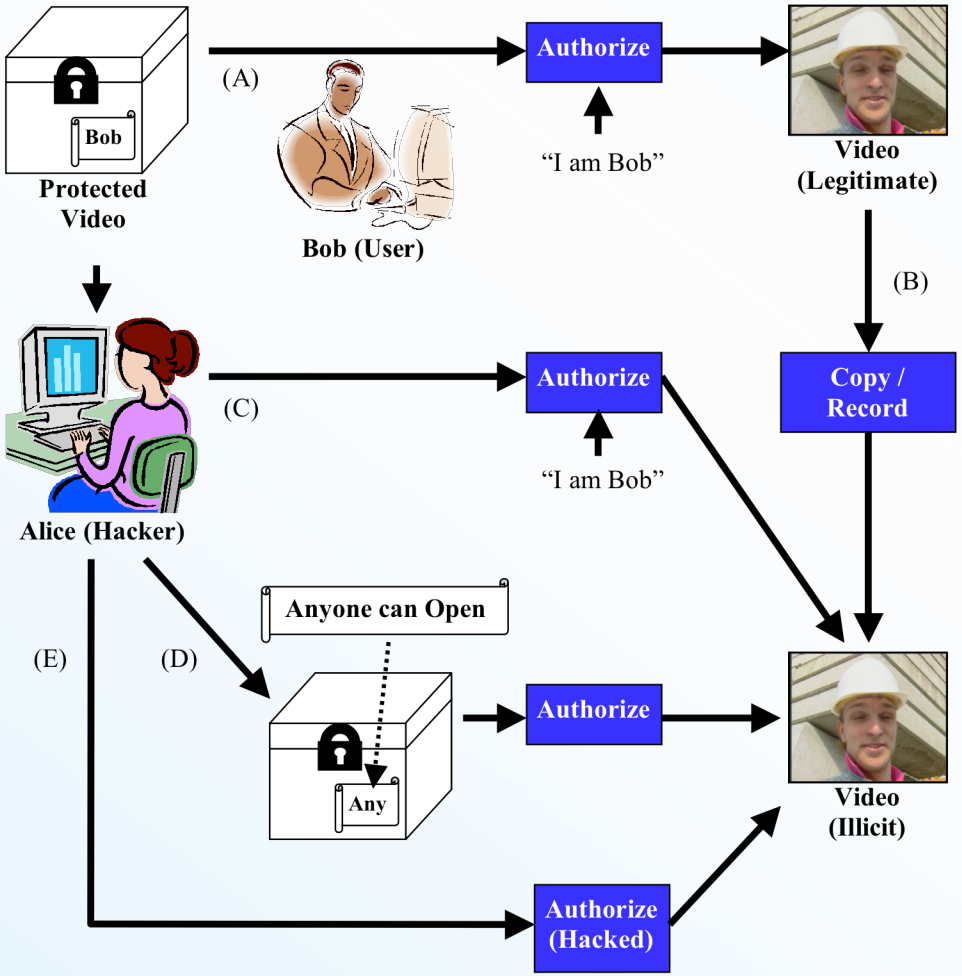


Legal Efforts

- Legal efforts
  - Digital Millennium Copyright Act (DMCA)
    - Anti-circumvention provisions
  - European Copyright Directive (EUCD)
    - Anti-circumvention provisions
    - Adoption has been slow
  - Consumer Broadband and Digital Television Promotion Act (CBDTPA)
  - Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003



A Content Protection System



(A) Standard Use

(B) Illicit copying or "analog hole"

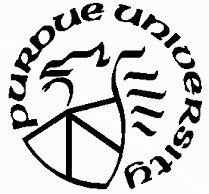
(C) False credentials

(D) Alteration of access conditions

(E) Use of "hacked" devices

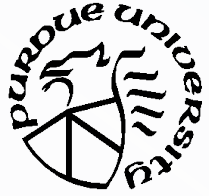
Users Concerns

- Users concerned that content protection systems may…
  - Unilaterally enforce usage rules that contravene the rights and privileges granted to the public
  - Violate expectations of privacy
  - Reduce competition amongst video / device vendors
  - Force users to pay increased costs to obtain content and devices that provide them with less control
    - Devices more complicated
    - Less compatibility or interoperability
  - Damage their devices (Sony's rootkit)



Multimedia Security - Tools Set

- **Encryption**
- **Authentication**
- **Hashing**
- **Time-stamping**
- **Watermarking**

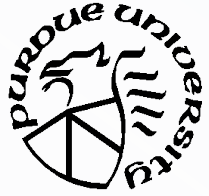


The New Battlefield!!

- **Books!**

DRM

- Stop working on this!!!
  - DRM systems face innovation of many attackers
  - Content protection system must remain secure for a long time -BUT attackers only need to succeed once
- A "technology" fix will not solve the mess we are in today
- The protection of intellectual property rights is perhaps one of the last major barriers in the "digital world"



What is THE important problem moving forward?

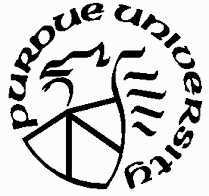
TRUST

Who and What I do trust?

- **People, Data, and Physical Things**
- **Done is plain sight!**
- **This is not just a technical problem**

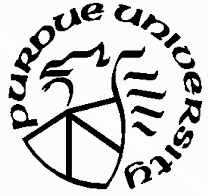
Important Application Domains

- **Authentication**
  - **People, data, and physical objects**
  - **Surveillance**
  - **Biometrics**
  - **“things” (rfid)**
- **Forensics**
  - **Data, e.g. Medical Imaging**
  - **Forgery of “events”**
  - **Content tracking**



Application Domains

- **Privacy**
  - **Remote Sensing**
  - **Databases (degradable content)**
  - **Mobile Systems and Sensor Networks**
    - **Sensors are everywhere**



What Are My Neighbors Doing?

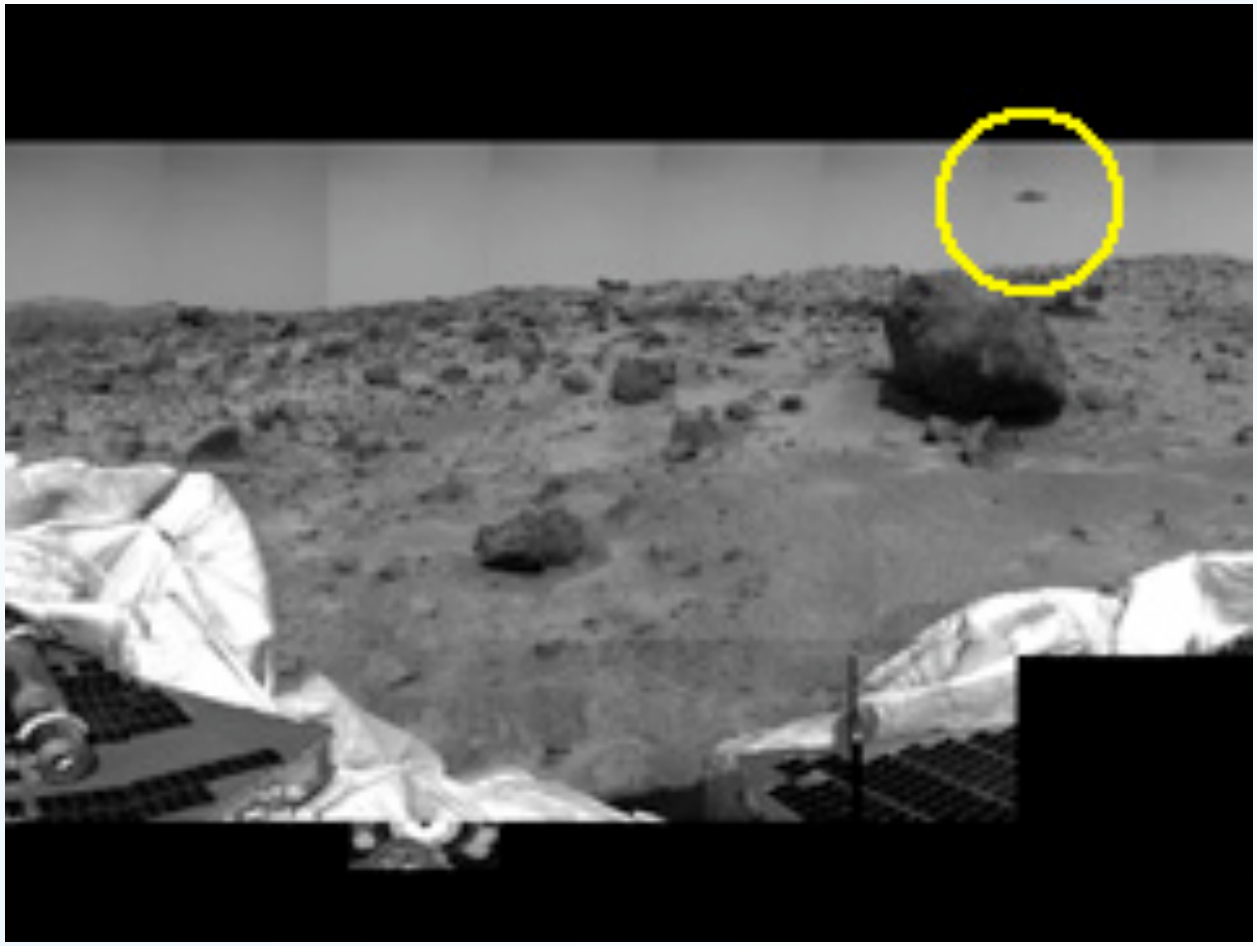
Where?

When?

Forensics


SPY
WHITE-HOT POLITICS ISSUE
KENNEDY
The Torch Passes
PLUS:
THOSE SURPRISING GORE GIRLS!

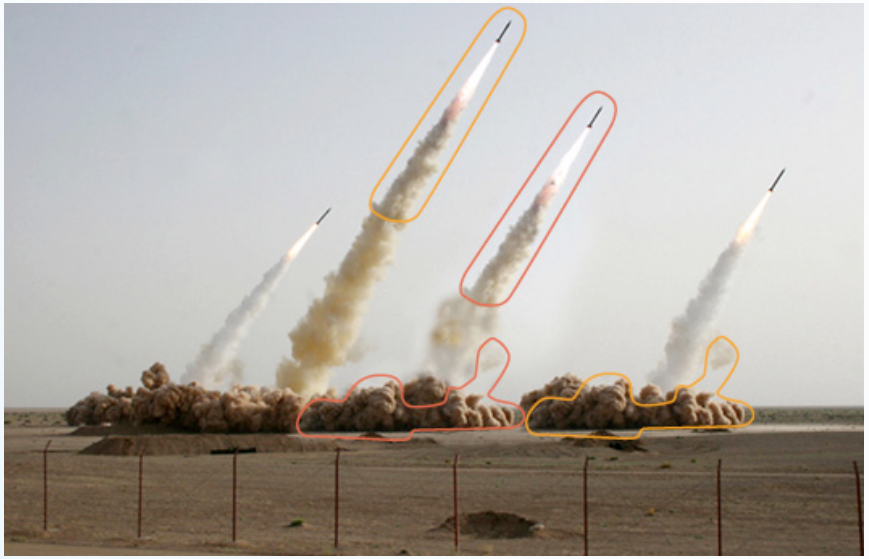
Forensics



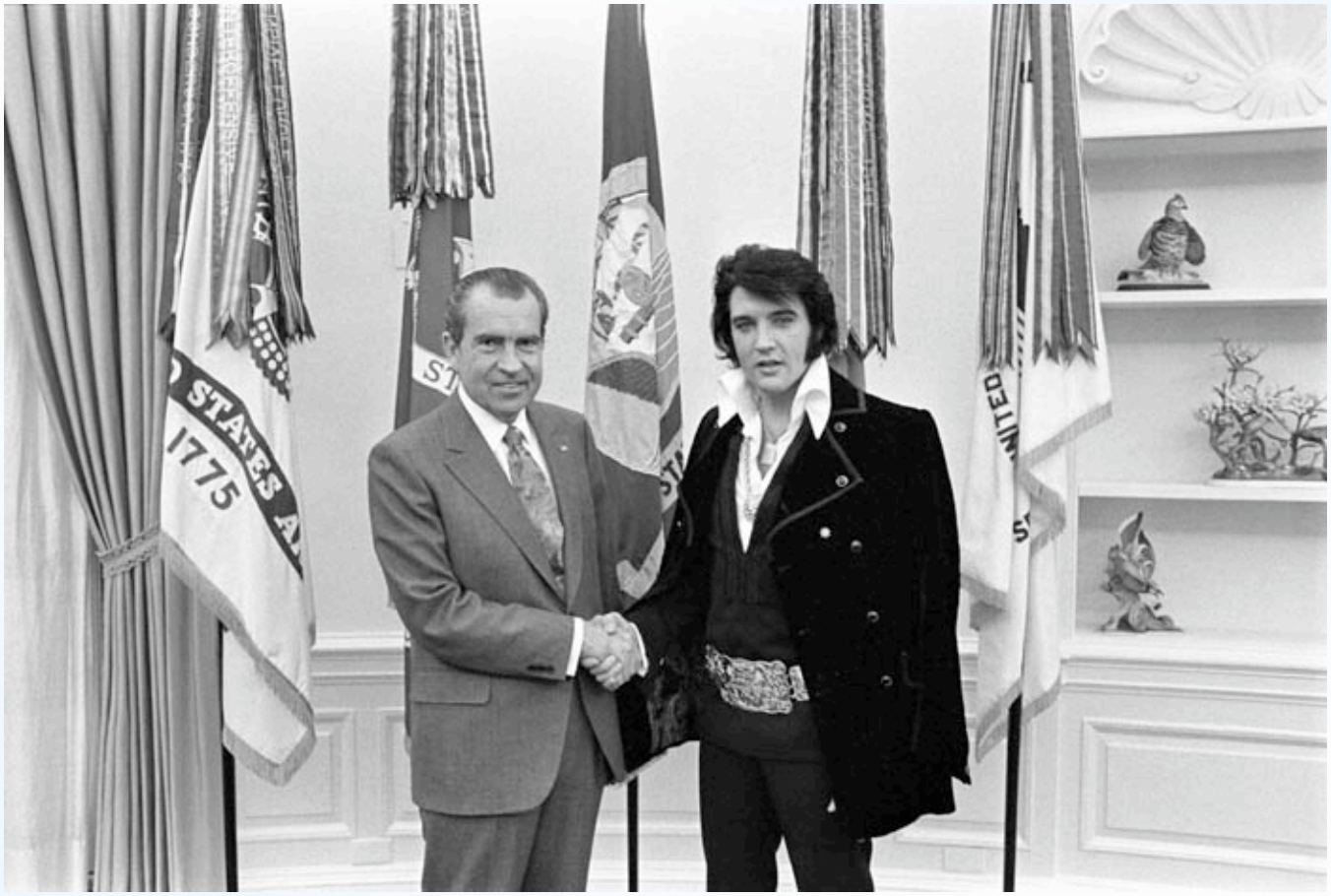
True or False?

July 10, 2008: Iranian Missiles Test

Well….well….well



Really!

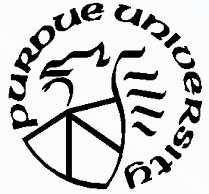


New Challenges

- **Authentication -**
  - **identity theft**
  - **mobile connected sensors**
- **Security, Surveillance, and Forensics**
  - **how do I protect information about myself?**
    - **rfid-like devices**
    - **tracking - e.g. who is in the parking lot?**
- **Scalable data conditional access - databases**
- **Use of context from the application**

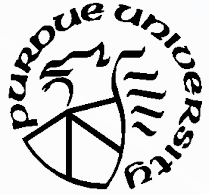
Sensor Forensics

- Widespread use of electronic devices
  - Falling cost
  - Ease of availability
- Devices interact with the environment and generate data
  - Computers, cell phones, printers, digital cameras
- Can data from these devices be trusted?
  - Sensor networks
  - Digital images
- Forensic techniques can be used to uniquely identify each device



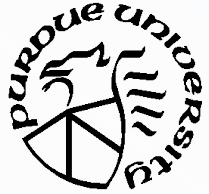
Sensor Forensics

- Forensic characterization
  - Observe device output ➔ which device produced it?
  - Exploit how the device "makes" its output
- Device authentication
  - Performed using forensic characterization
  - Identify device type, make, model, configuration
  - Can the sensor be trusted?
- Detection of data forgery or alteration
- Fingerprint and trace



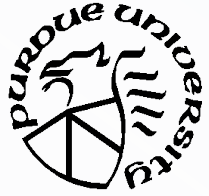
Signatures

- ***intrinsic signature*** **- identity as much information as possible from output of the device**
- **Embed auxiliary information in output via *extrinsic signature***
- **Intrinsic and extrinsic signatures are based on the basics of how the device operates**



Sensor Forensics Research

- **Printers**
- **Cameras**
- **Scanners**
- **Sensors Nodes**
- **RF Devices**

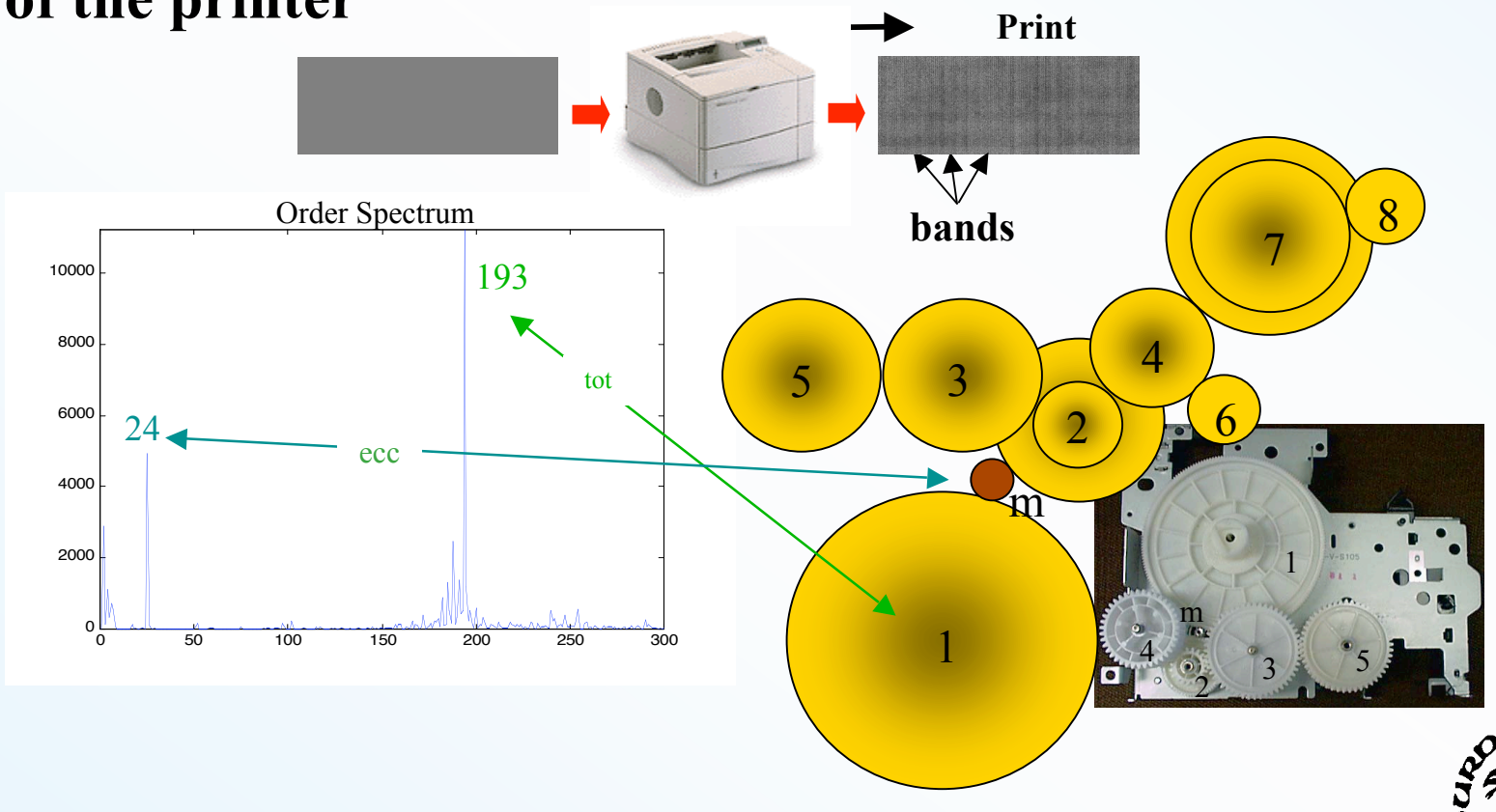


Sensor Forensics

www.sensor-forensics.org

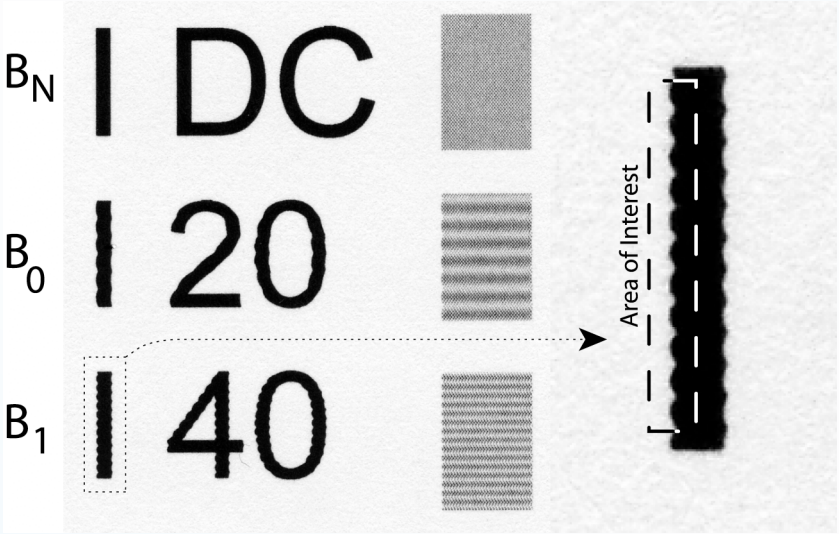
Printers

- **Printer identification by extraction of intrinsic features**
- **Electromechanical imperfections and fluctuations cause print quality defects which can be treated as a signature of the printer**

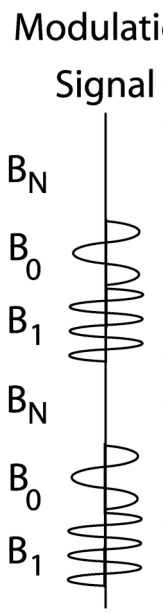


Effects of Laser Modulation

- *Artificial banding* in midtone regions
  - Can be minimized by designing the modulation signal to lie below the human contrast sensitivity curve
- Edge raggedness visible on vertical edges
  - Can be minimized by limiting embedding amplitude
  - Can also be used to detect the signals! Use ISO-13660 raggedness measure



Embedding Framework



is fashion, you. I had a steps unlike patrongly upon his of an evidence." "It yebrown secrecy was hair suggested. morning. "It is Sherlocked that them it, when yourself clearned it in the slipper name ever her on the leventual important,

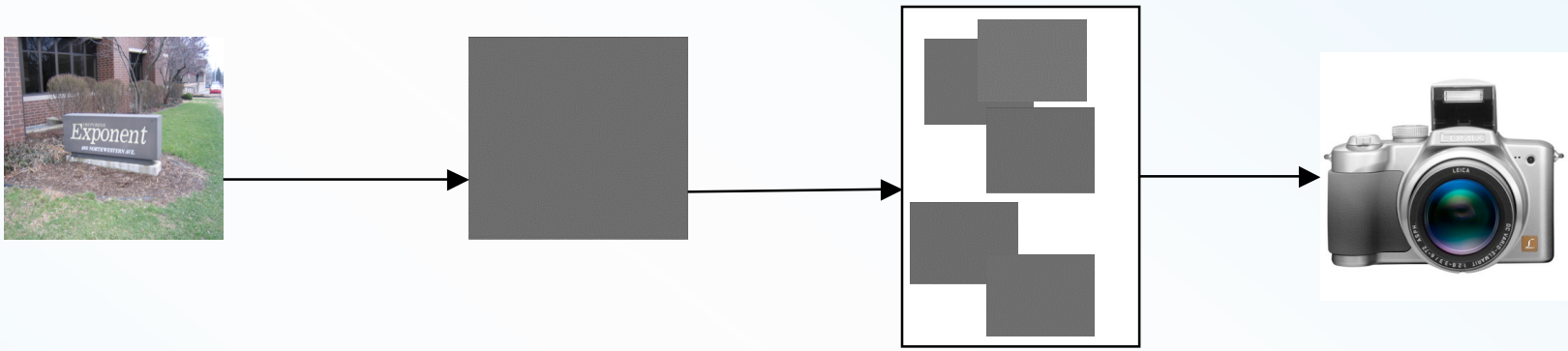
Sensor Based Characterization

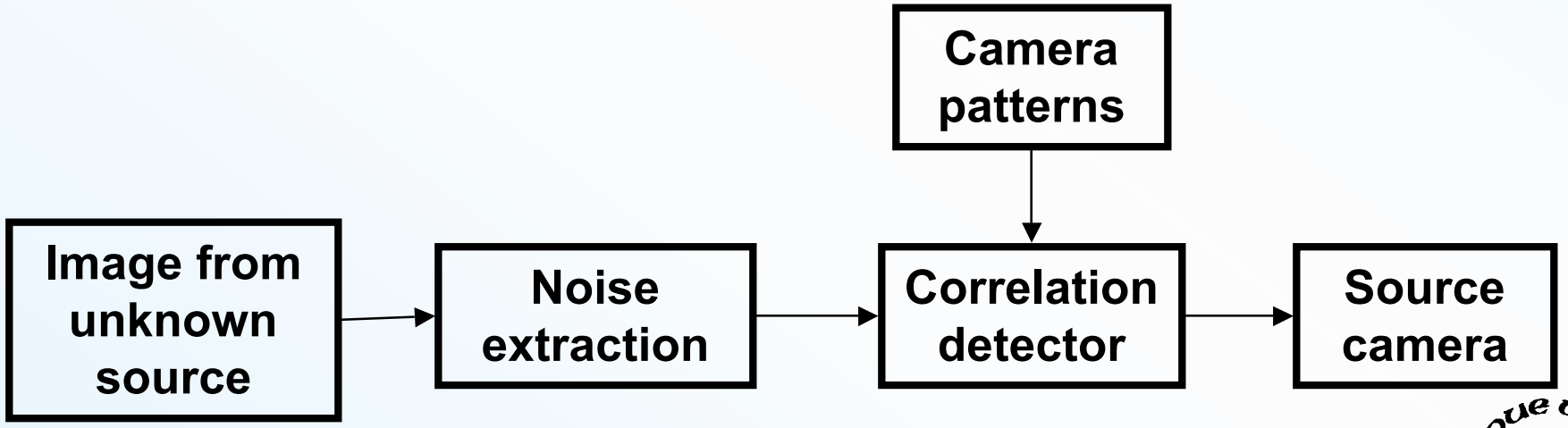
- **Two geometries of imaging sensors**
  - **Two dimensional (Cameras)**
  - **One dimensional (Flatbed Scanners)**
- **Noise pattern in imaging sensor is highly correlated to manufacturing defects**
  - **Fixed Pattern Noise (FPN) and Photo-Response Non-Uniformity (PRNU)**
  - **Noise modeled as the sum of random and fixed components**
- **Fixed component used for image source identification**

Sensor Based Characterization

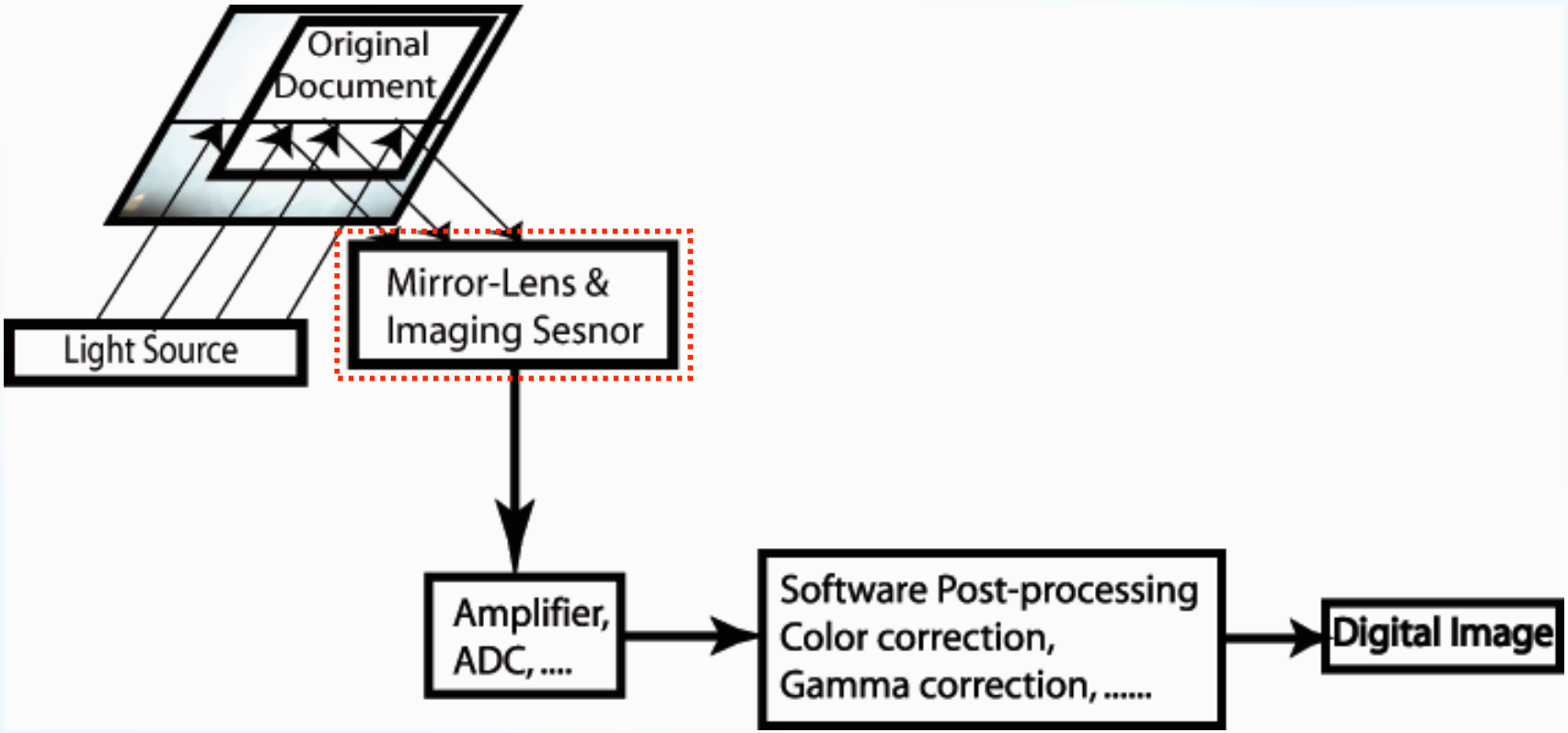
- **Pattern noise used as sensor reference pattern**
  - **Estimated using a denoising filter bank**
- **For scanners, the linear array is translated to generate the image ➔ periodicity in the fixed pattern noise corresponding to different rows of the scanned image**
- **No similar correlation between fixed pattern noise corresponding to different columns of the scanned image**

Source Camera Identification

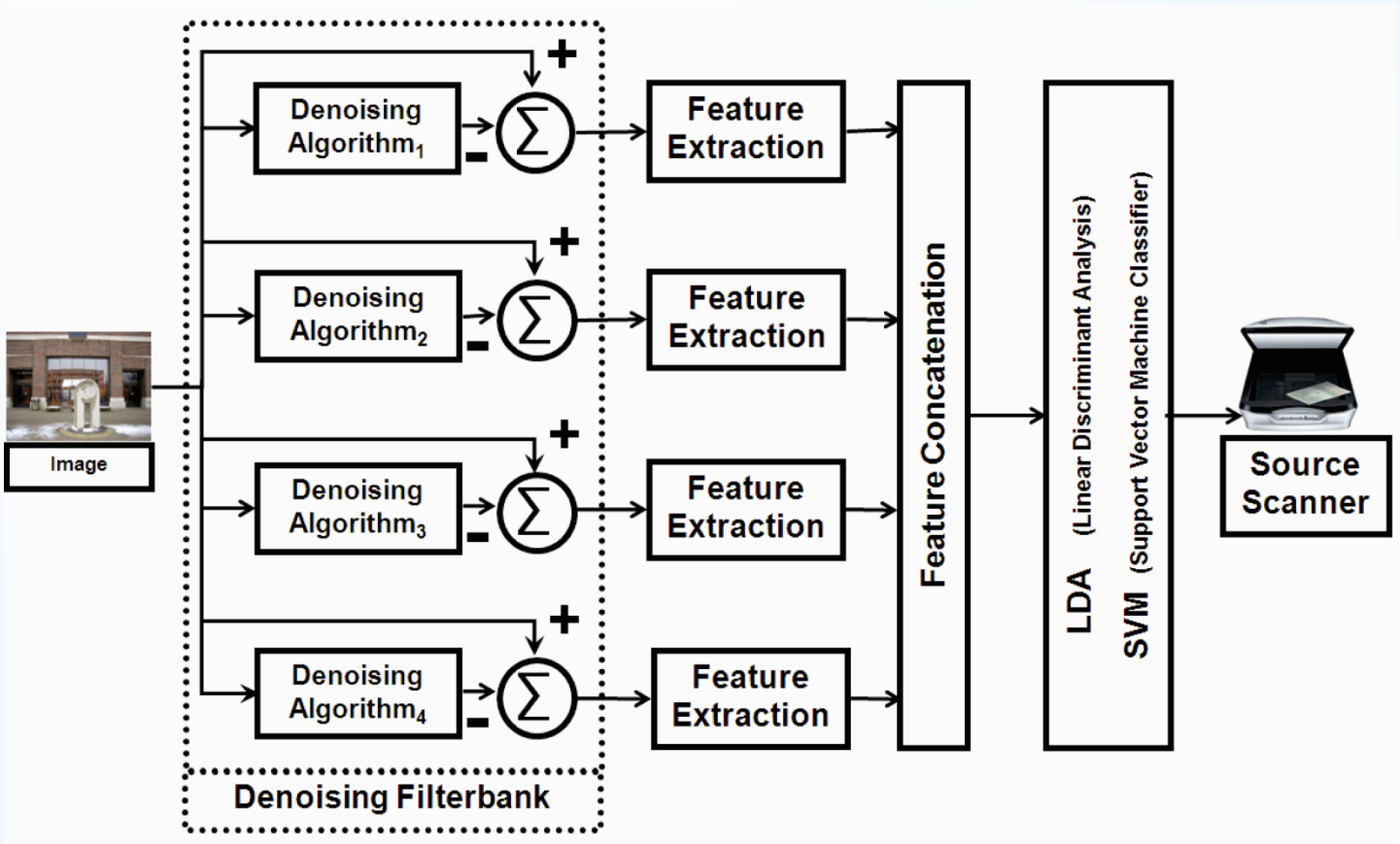




Flatbed Scanner Imaging Pipeline



Source Scanner Identification



Conclusion

We are having fun!

Multimedia Security: A Viewpoint From A Walking Wounded

Edward J. Delp

Video and Image Processing Laboratory(*VIPER*)
School of Electrical and Computer Engineering
School of Biomedical Engineering
Purdue University
West Lafayette, Indiana

email: ace@ecn.purdue.edu

http://www.ece.purdue.edu/~ace