Sensor-level Privacy for Thermal Cameras

Francesco Pittaluga
Aleksandar Zivkovic
Sanjeev J. Koppal

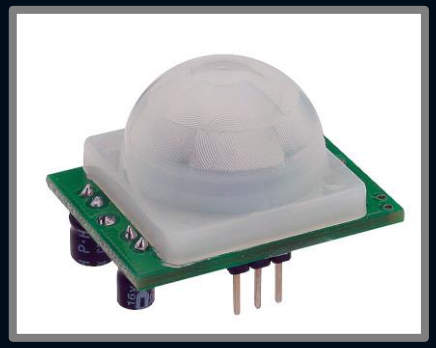
University of Florida

Imaging and Tracking People

Surveillance

Military

Gaming



IoT

Mobile

Balancing Privacy and Utility

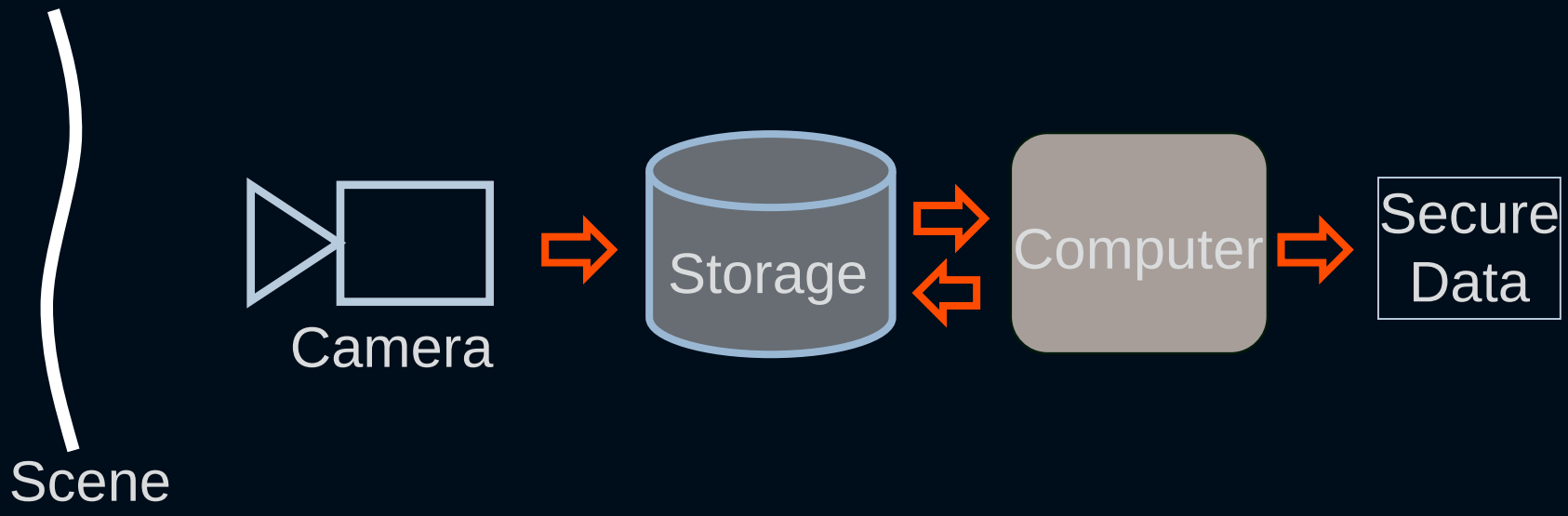
Hospitals

Schools

Retirement homes

Workplaces

Conventional Privacy Processing

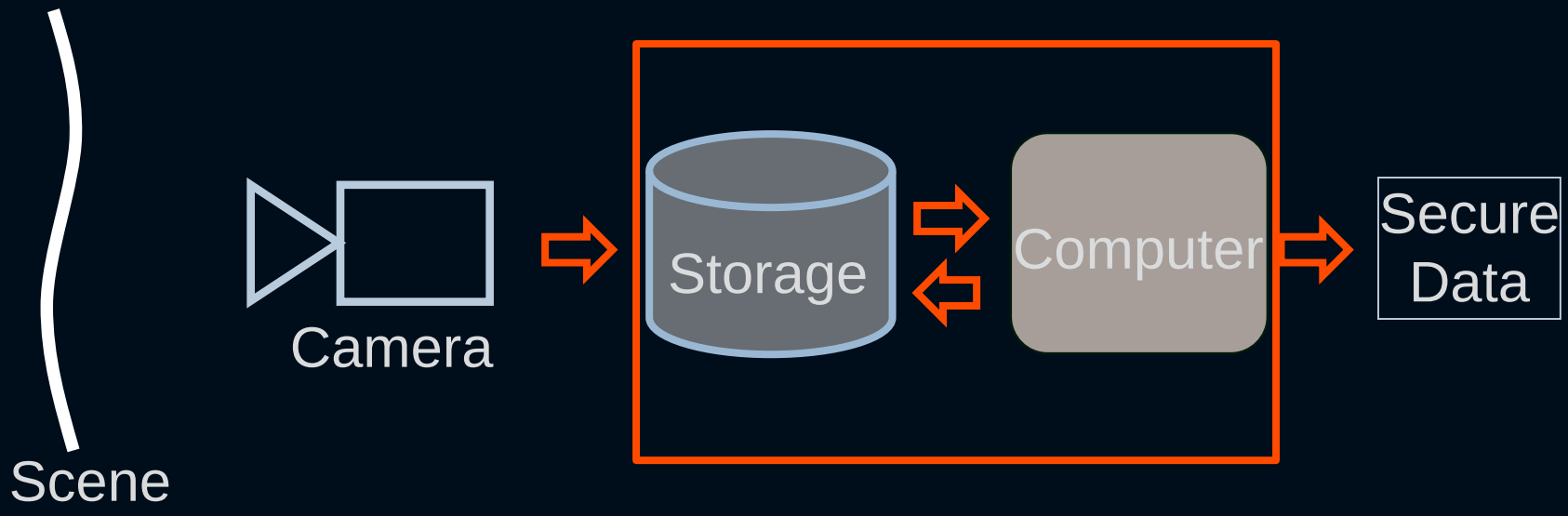


Post-capture processing

- Lock data with cryptography
- Edit images computationally

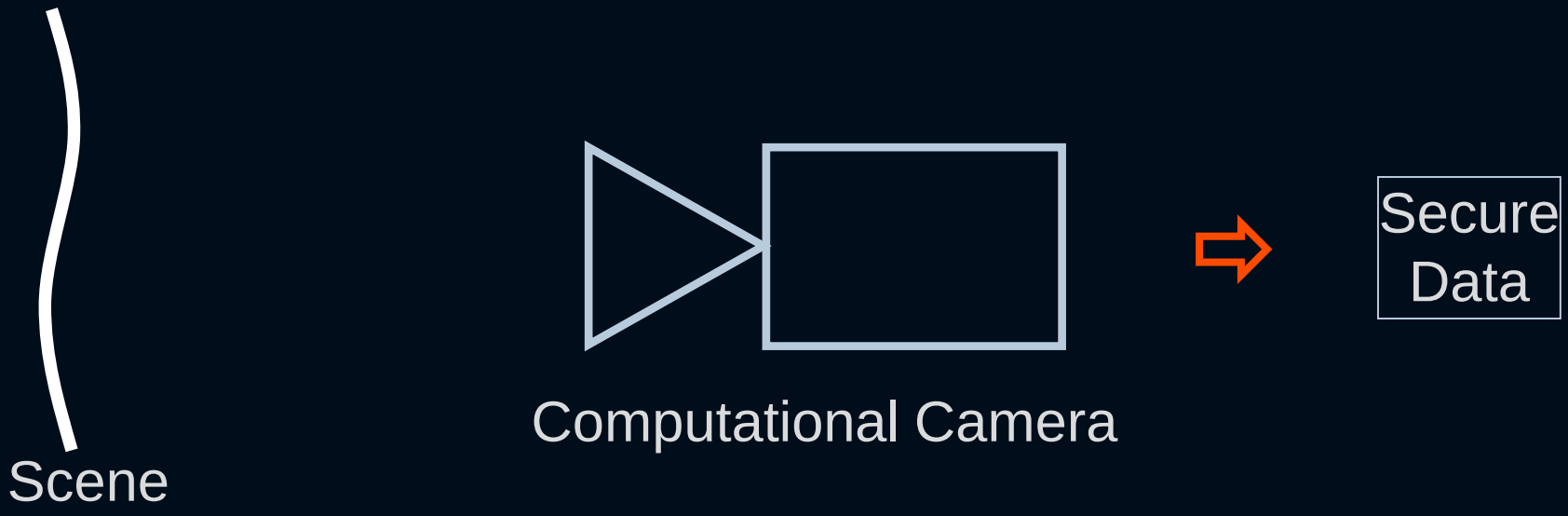
Boyle 2000, Sweeney 2002, Johnson et al. (IETF) 2003, Gross et al. 2009, Agrawal and Narayanan 2011, …

Conventional Privacy Processing



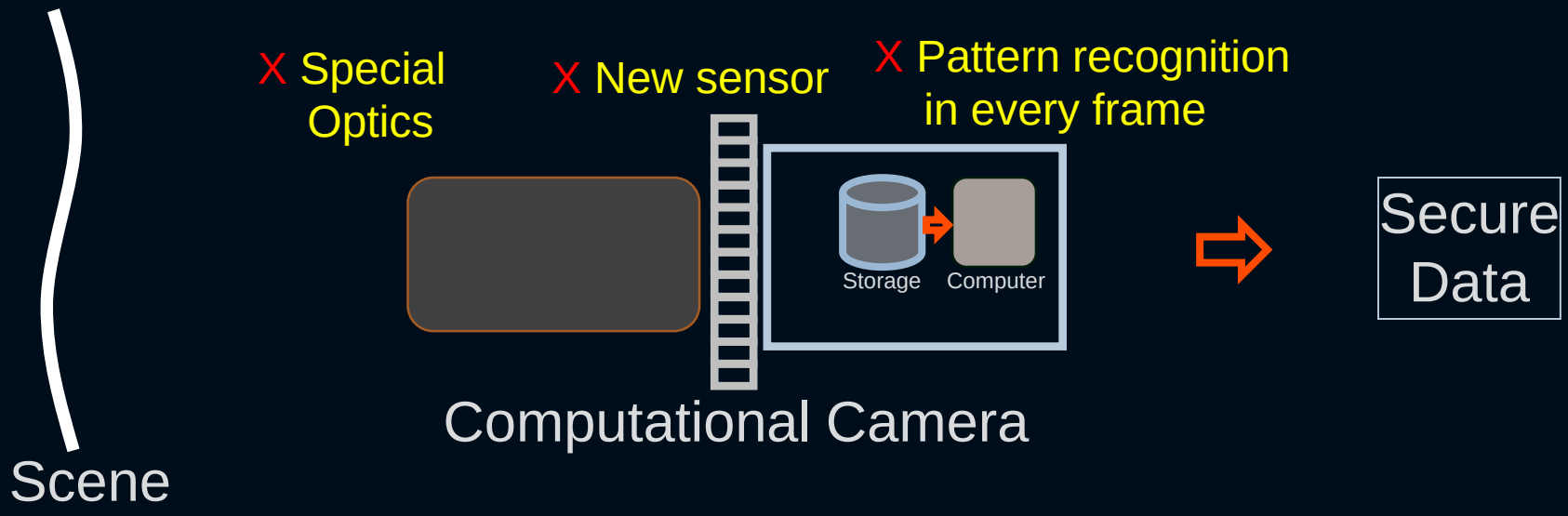
Post-capture strategy has an inherent vulnerability

Privacy Preserving Computational Cameras



Only capture light-field samples that are needed

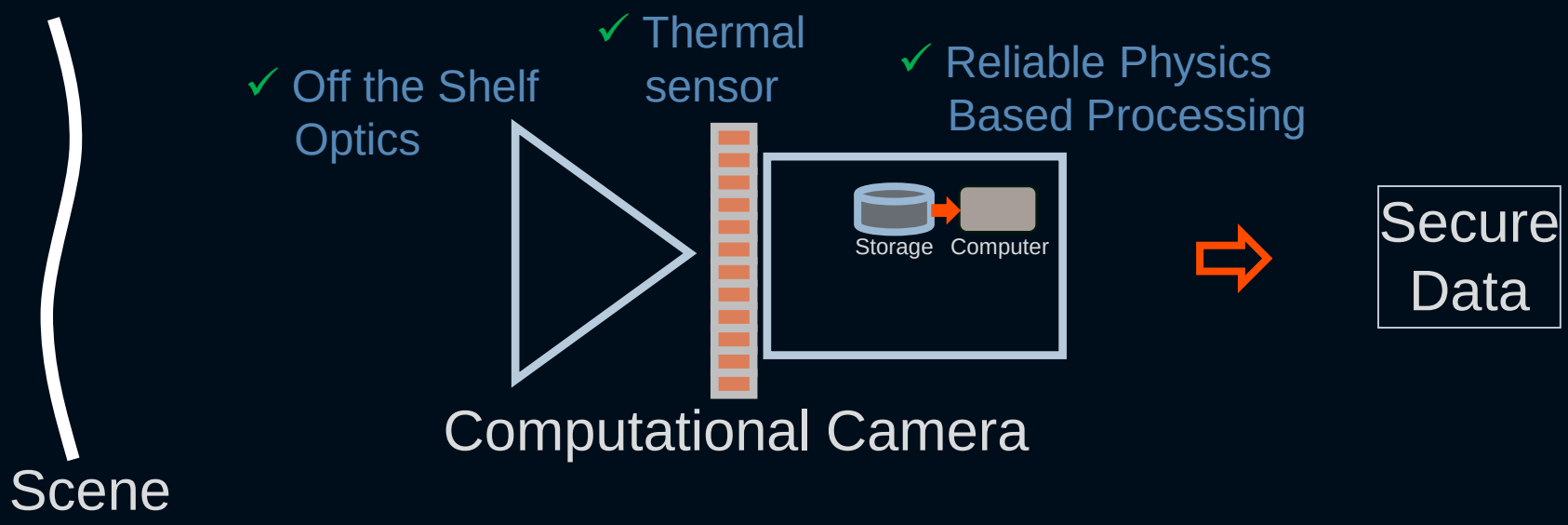
Computational Camera: Three Approaches



Three Problems ⇨ Limited Adoption

Nelson et al. 2005,Winkler et al. 2014, Fernandez-Berni et al. 2014
Zhang et al, 2014, Pittaluga and Koppal 2015
Chattopadhyay and Boult 2007, Winkler and Renner 2010, Narayanan and Mrityunjay 2011

Our Idea: Sensor-level Privacy for Thermal Cameras

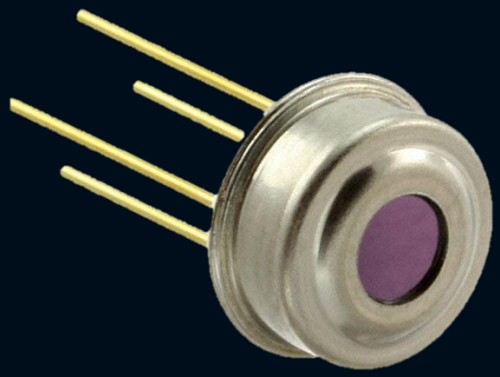


Our idea: use a *thermal* sensor

(Wavelengths > 3μm)

Thermal Cameras are Coming Soon!

FLIR One 80x60
~$250

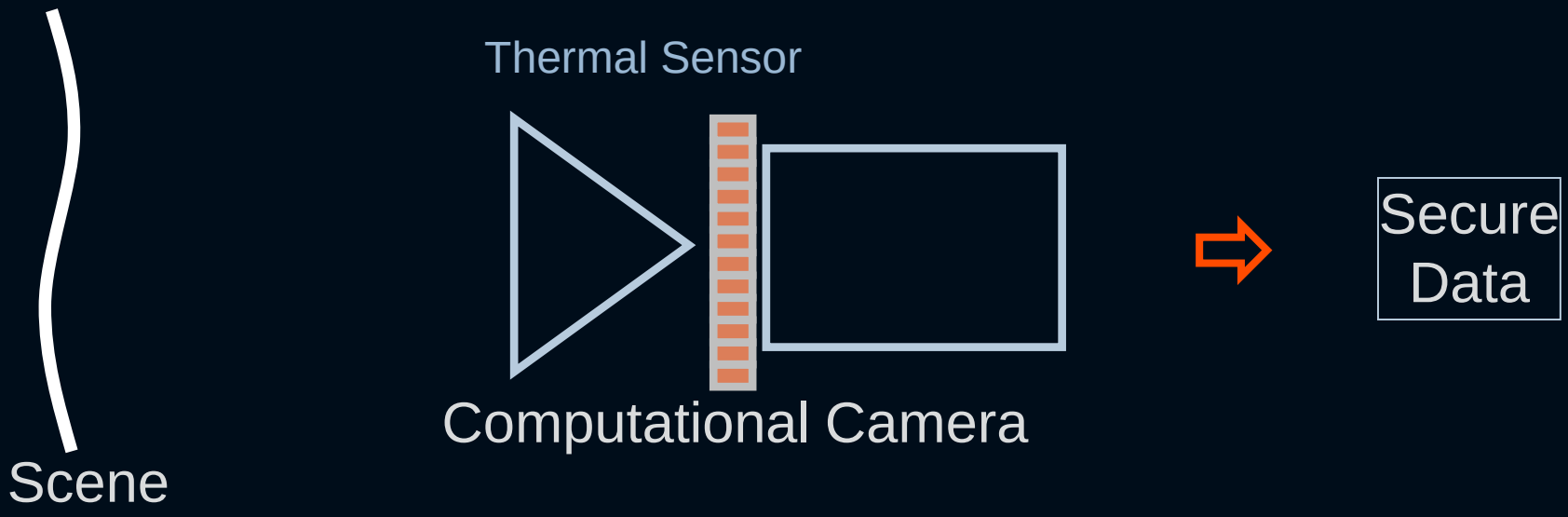


Melaxis 16x4
~$75

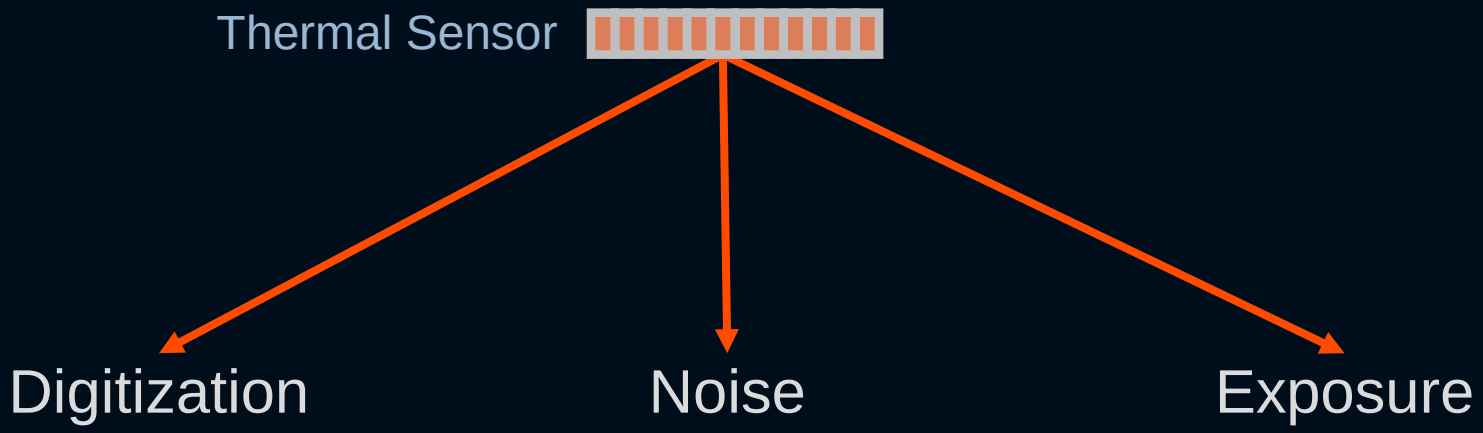
FLIR A6751SC

- Thermal cameras are not exotic anymore
- Thermal face recognition works

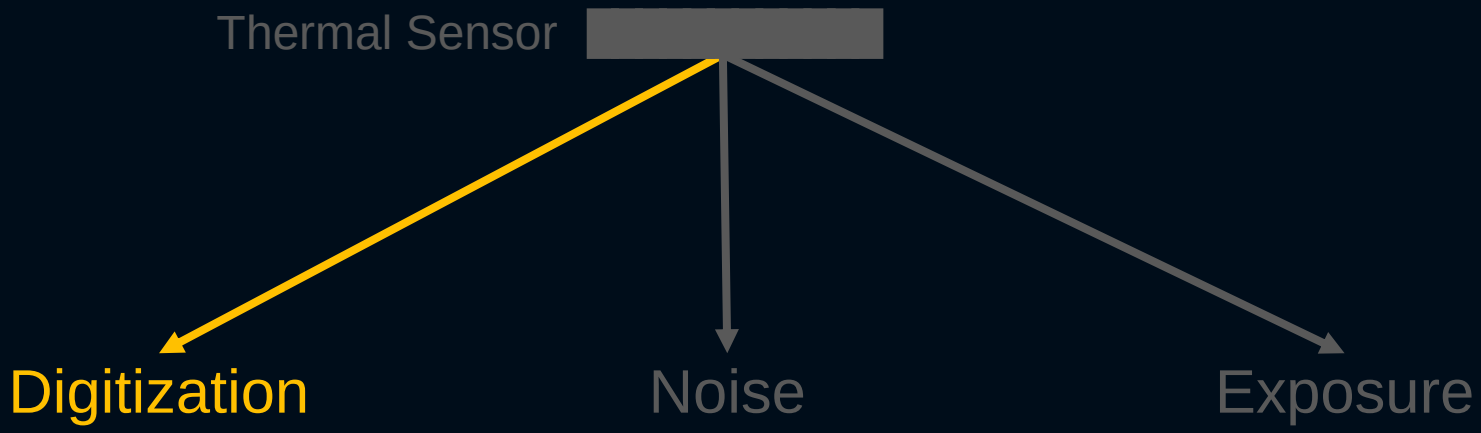
Three Sensor Level Approaches



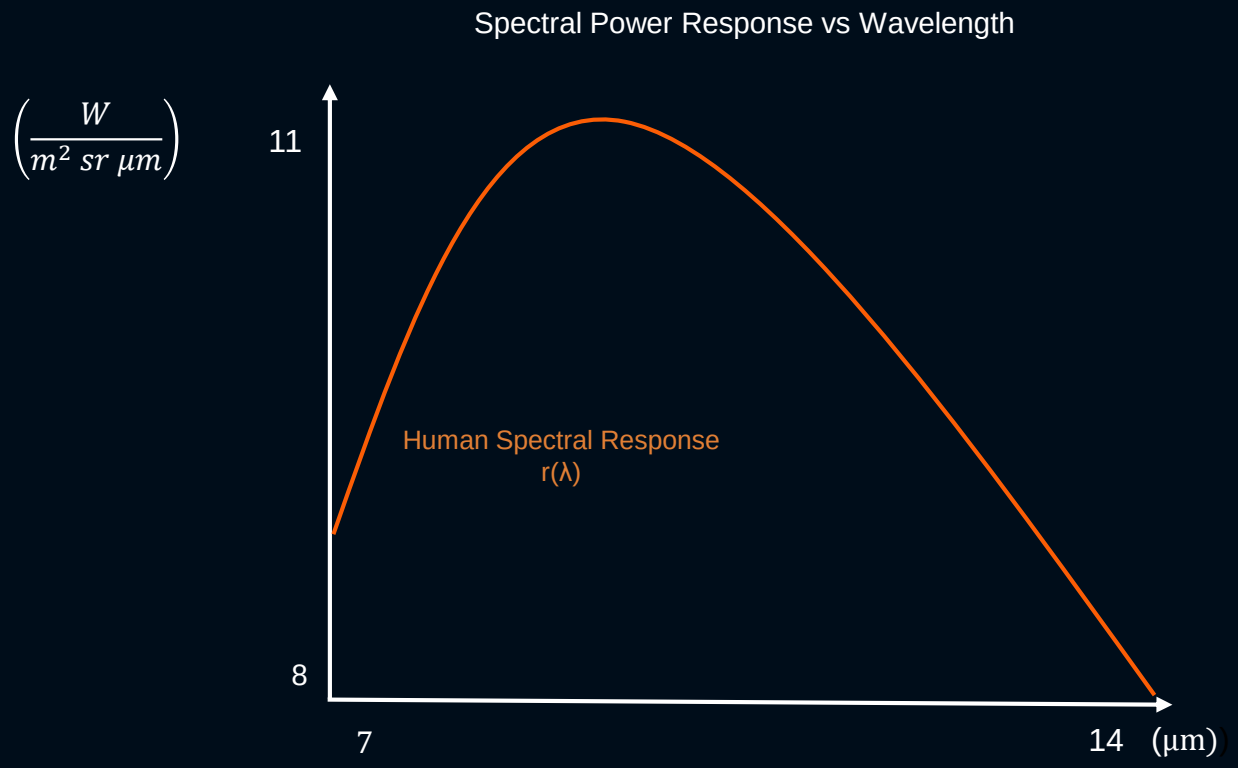
Three Sensor Level Approaches



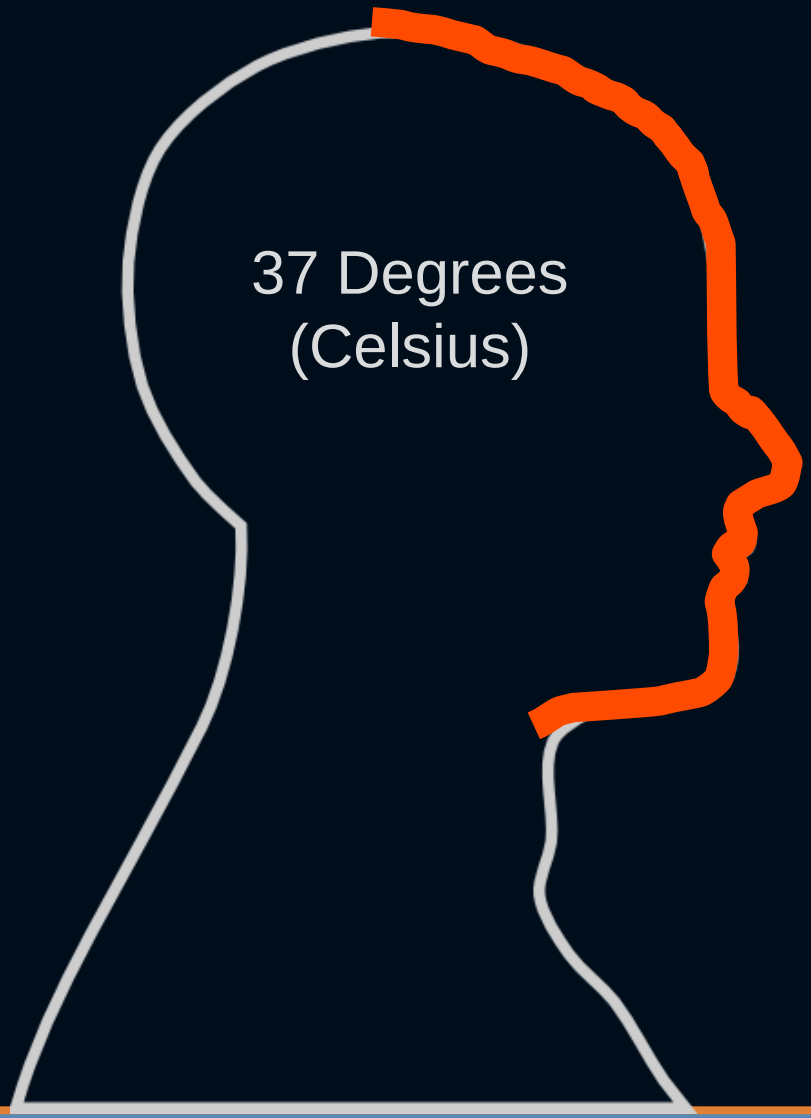
Three Sensor Level Approaches



Humans are broadband



Facial skin temperature reaches an equilibrium

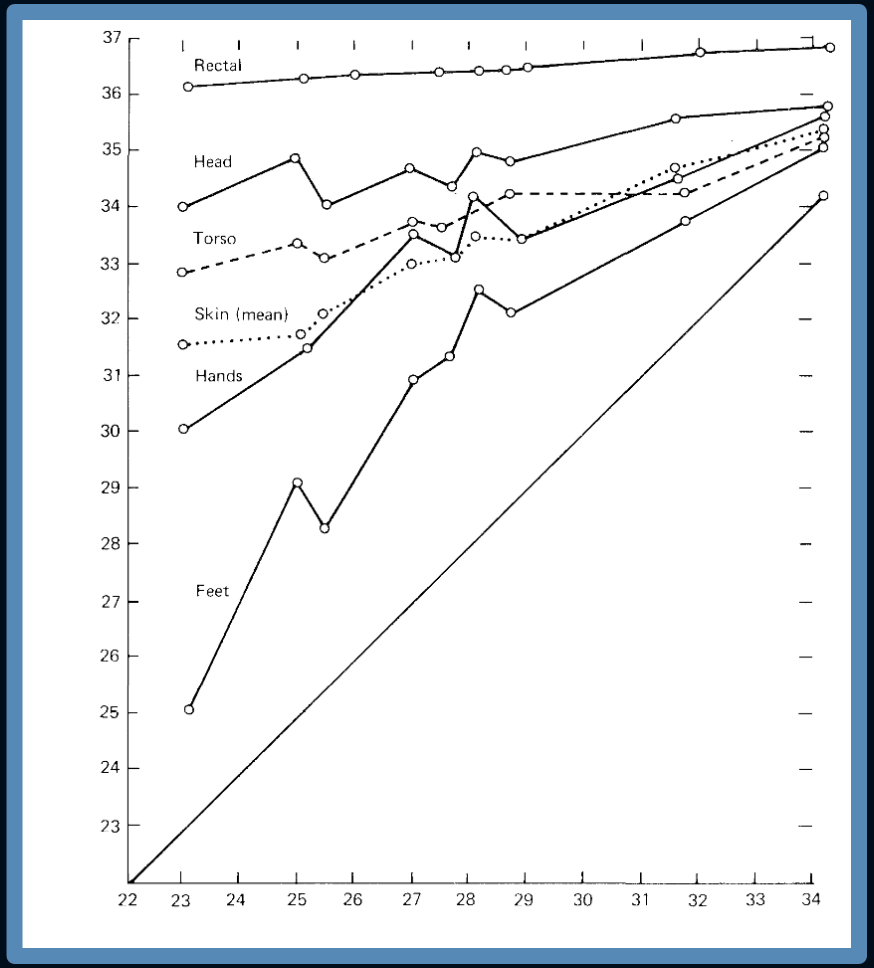


Outside temperature known
= T Celsius

Facial skin temperature *F* (T, 37)

This mapping is known

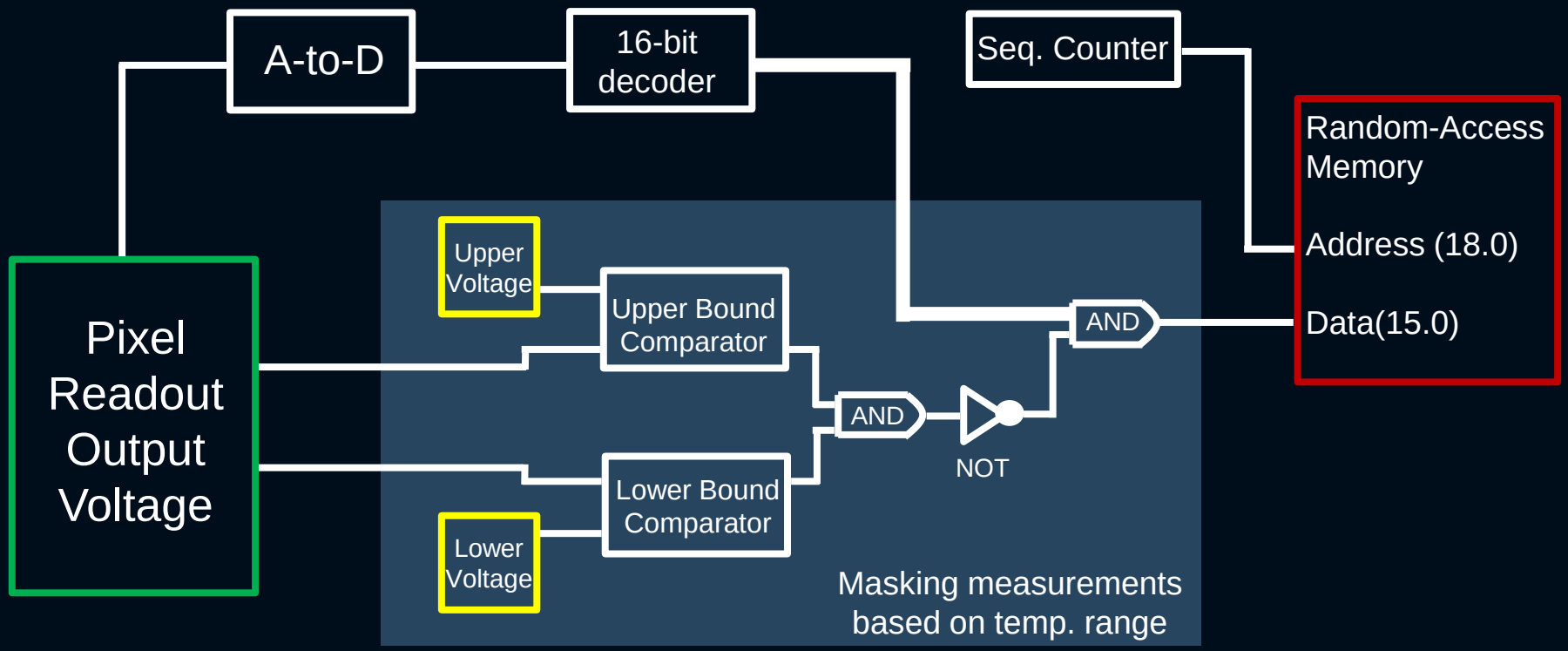
Skin Temperature °C



Ambient Temperature °C

Olesen and Parsons 2002

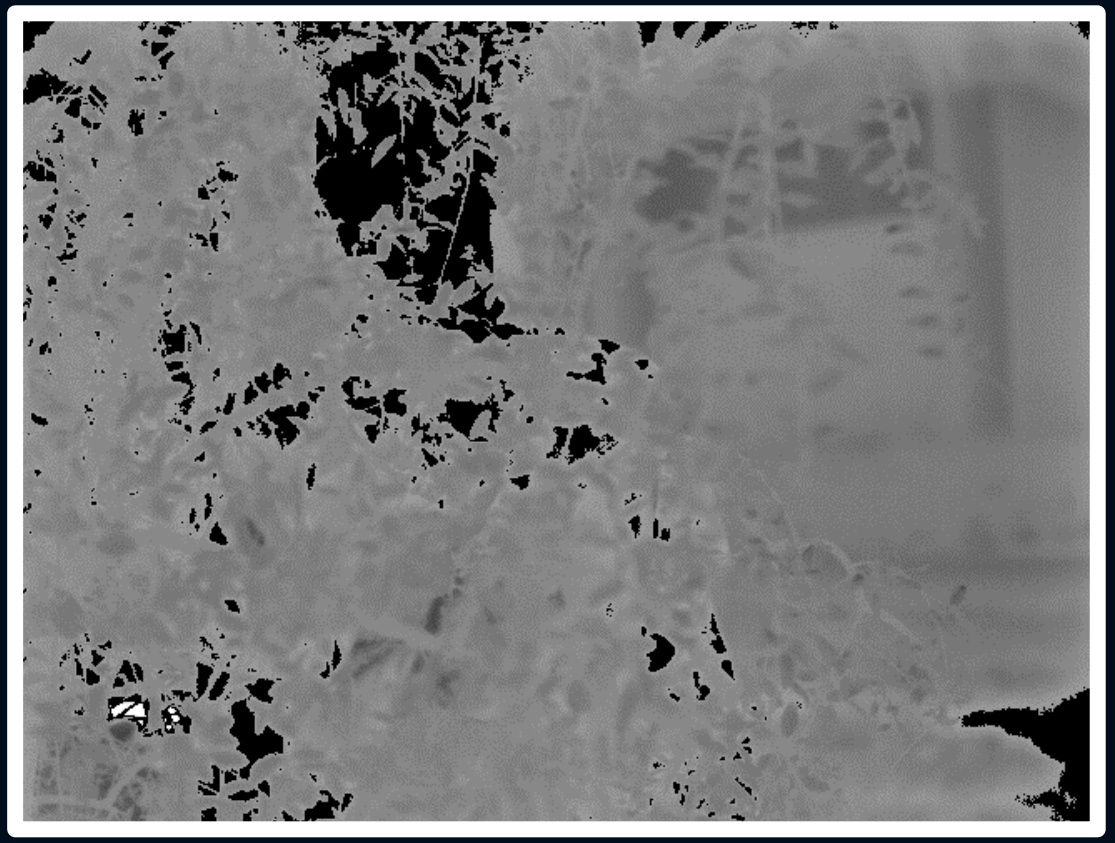
Removing pixels in this range during digitization



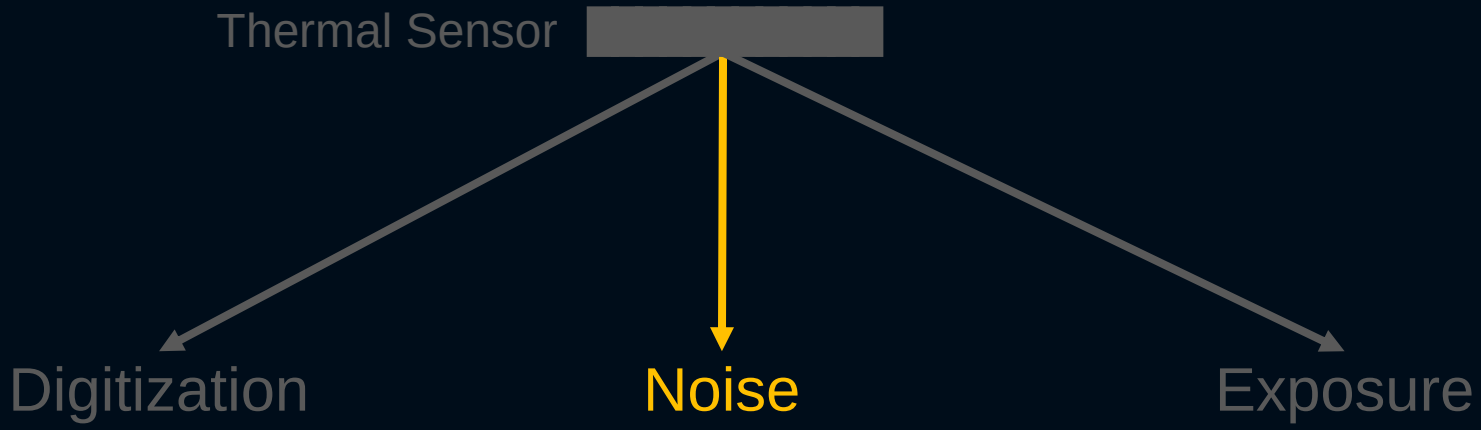
ASIC Modification

Digitization Result

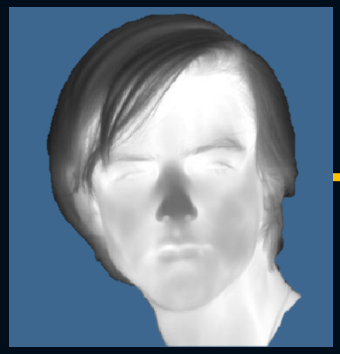
Digitization Result



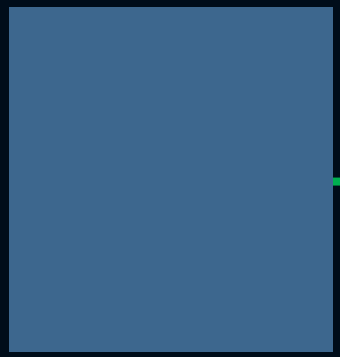
Three Sensor Level Approaches

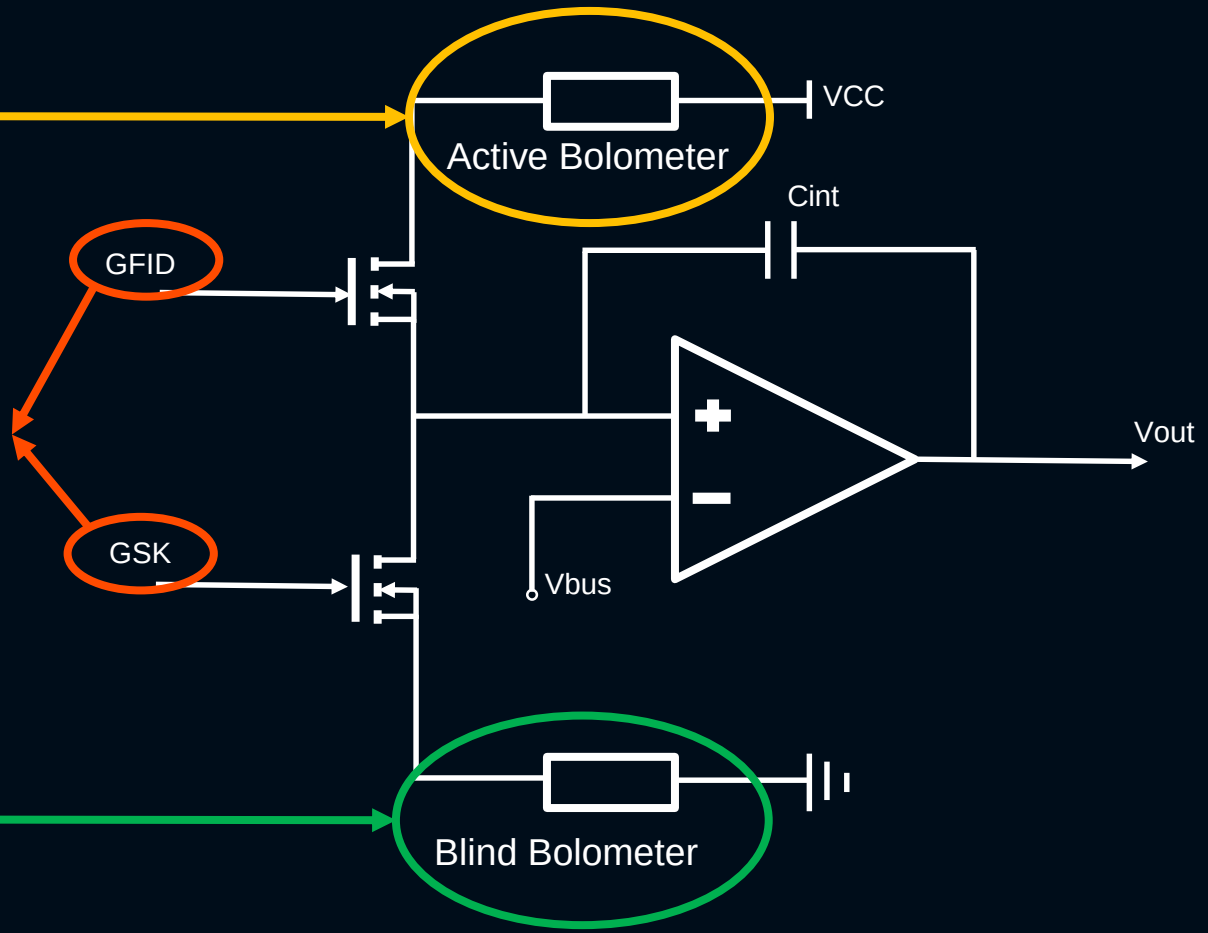


Adding noise to the bolometer

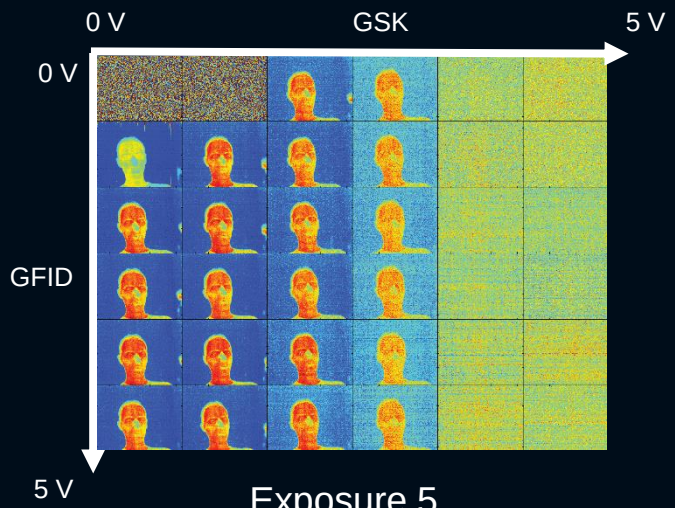


Tunable Bias Voltages

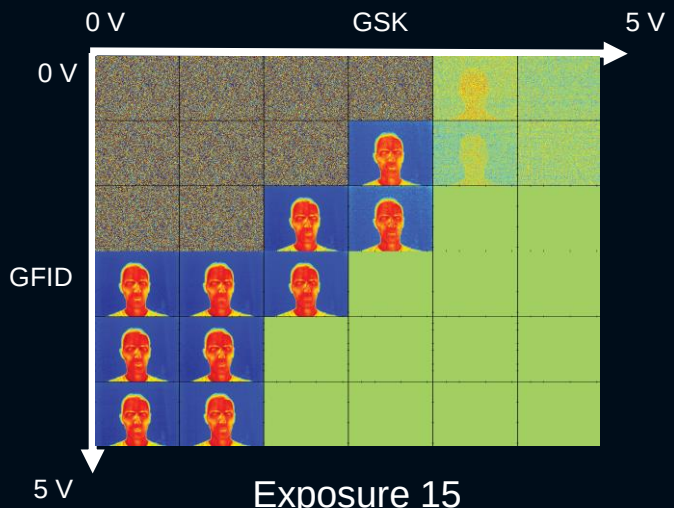




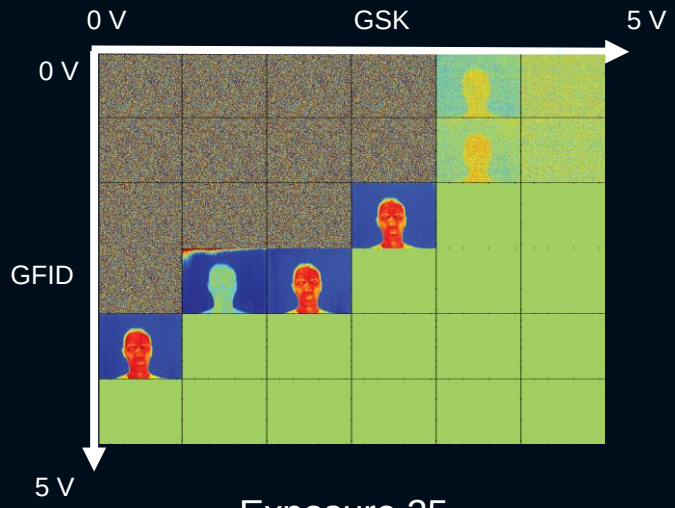
The effect of bias voltages



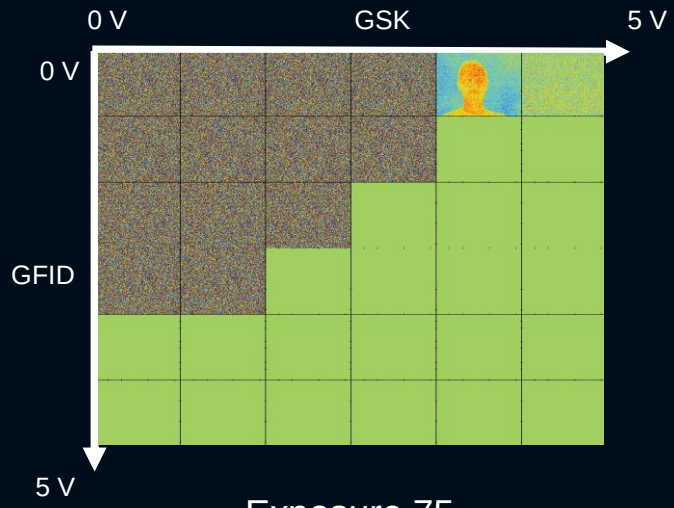
Exposure 5



Exposure 15

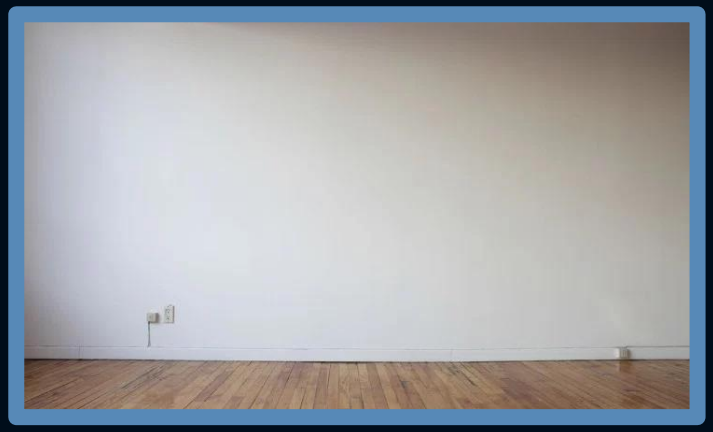


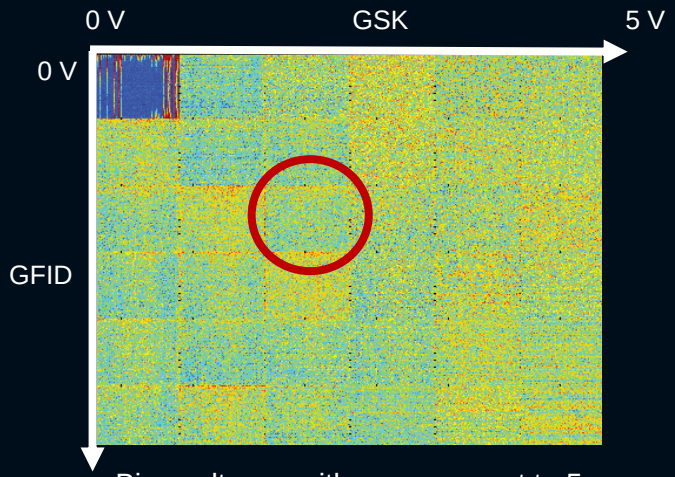
Exposure 25



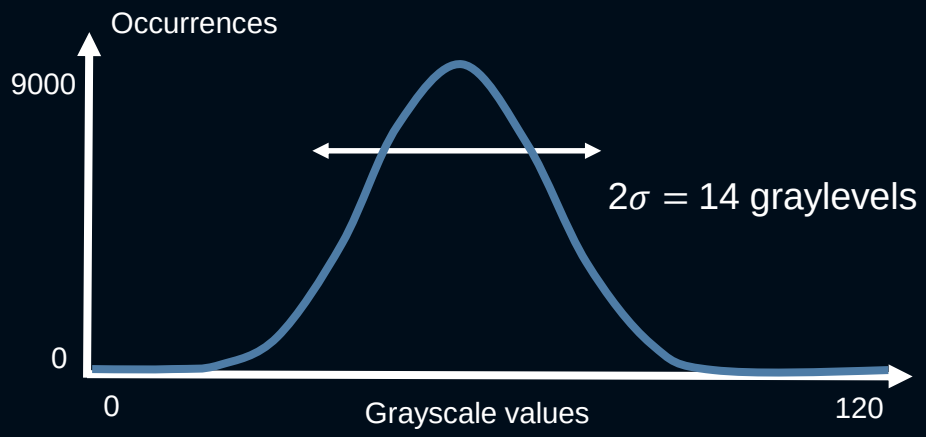
Exposure 75

Calibrating for noise and privacy





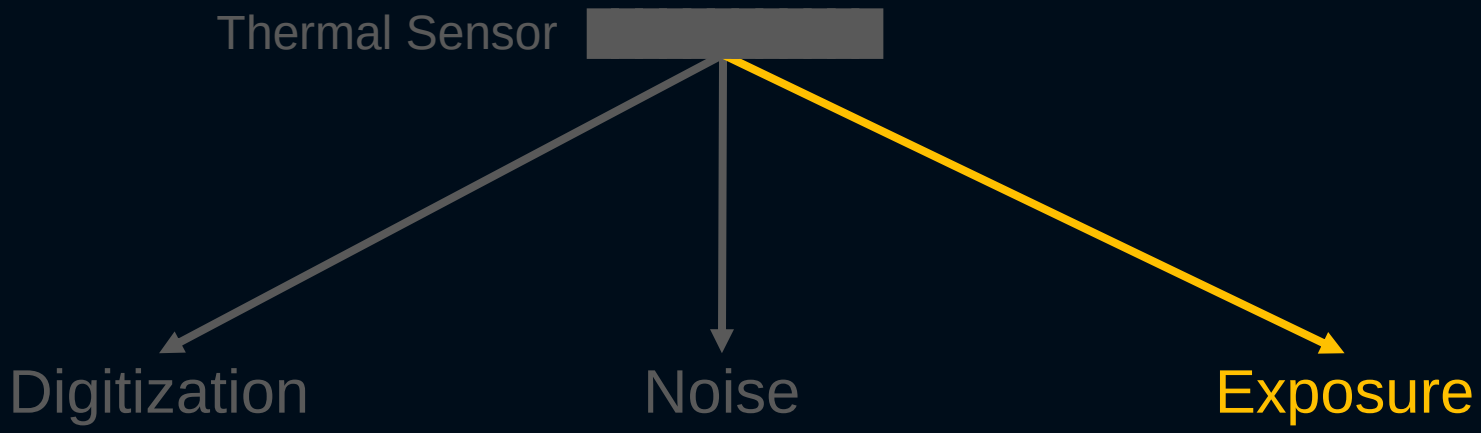
Bias voltages with exposure set to 5
For a flat lambertian plane



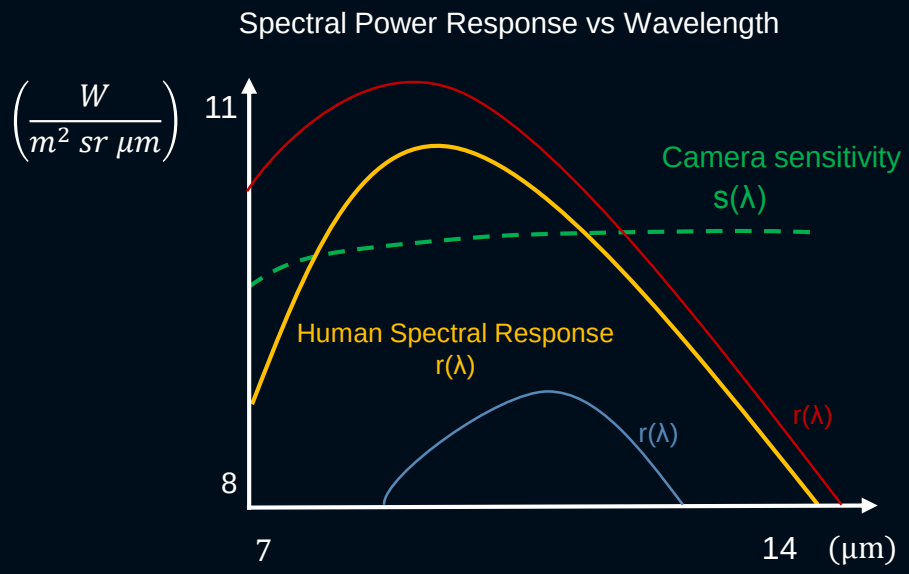
Histogram of values for the highest standard deviation

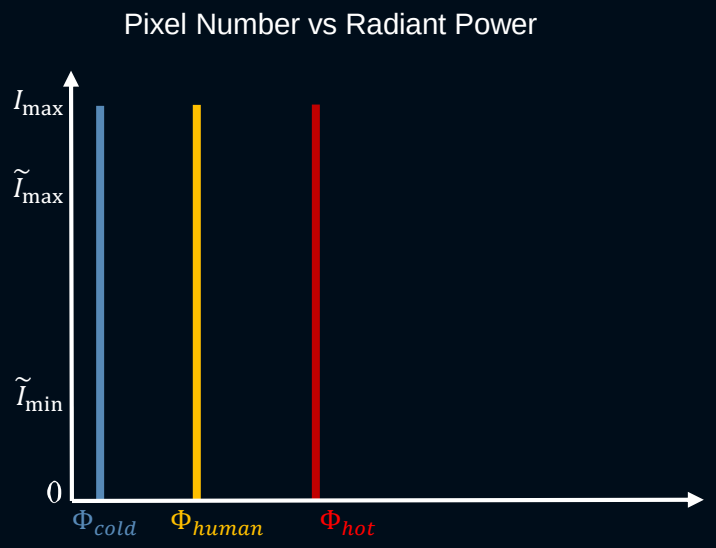
Noise Result: Head Tracking

Three Sensor Level Approaches



Temperature and radiant power

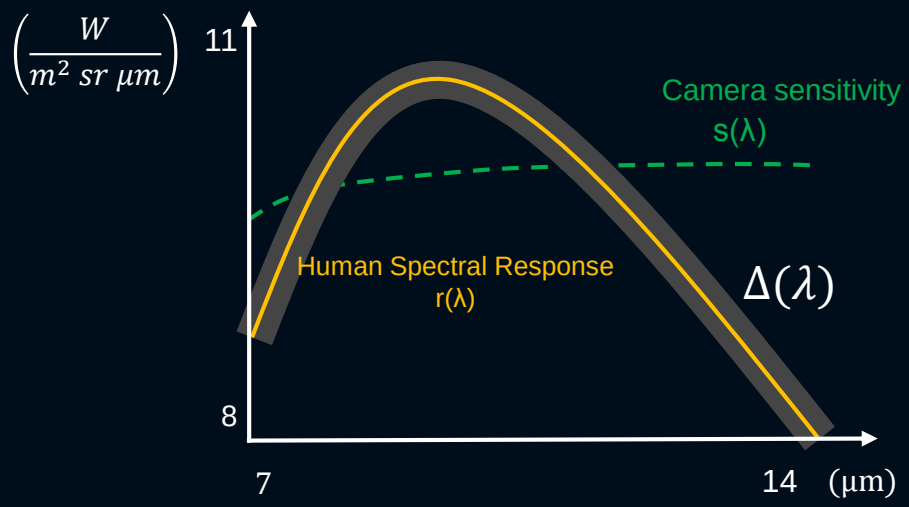




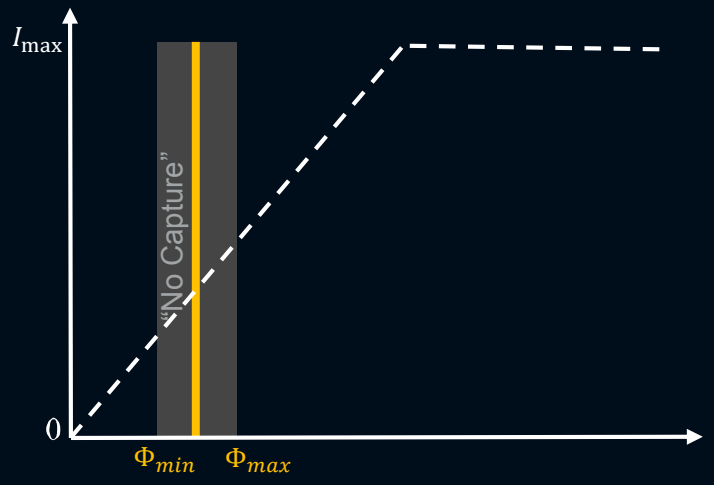
$$\Phi = \int_{\lambda_t}^{\lambda_h} s(\lambda) r(\lambda) d\lambda$$

No capture region

Spectral Power Response vs Wavelength



Pixel Number vs Radiant Power

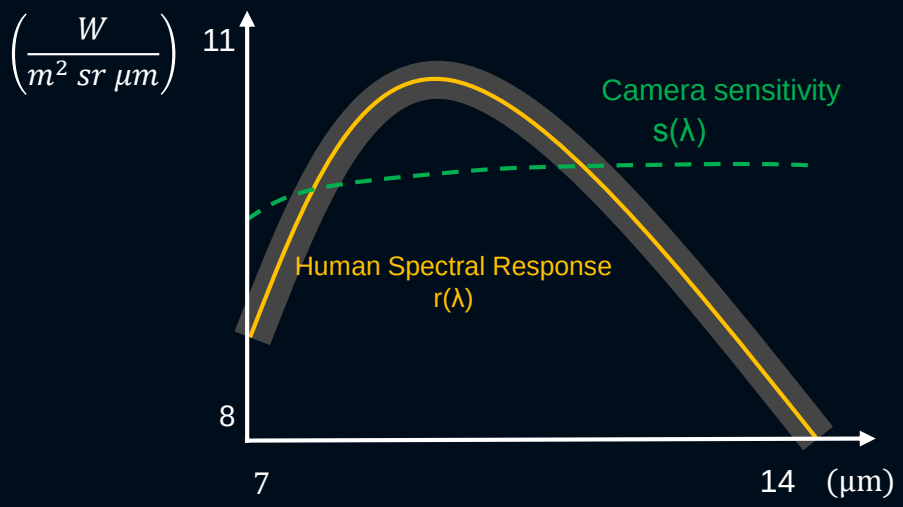


$$\Phi_{min} = \int_{\lambda_t}^{\lambda_h} s(\lambda)[r(\lambda) - \frac{\Delta(\lambda)}{2}]\, d\lambda$$

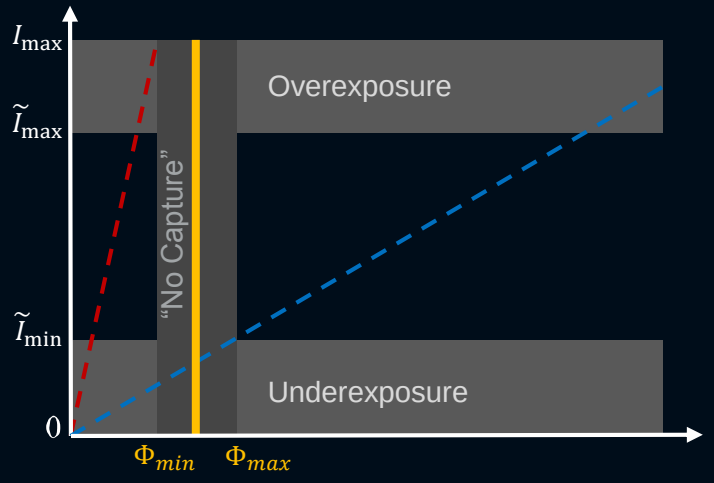
$$\Phi_{max} = \int_{\lambda_t}^{\lambda_h} s(\lambda)[r(\lambda) + \frac{\Delta(\lambda)}{2}]\, d\lambda$$

Exposures that remove no capture region

Spectral Power Response vs Wavelength



Pixel Number vs Radiant Power



Human Overexposed

$$t \geq \frac{g\tilde{I}_{max}(g)}{\Phi_{min}}$$

Human Underexposed

$$t \leq \frac{g\tilde{I}_{min}(g)}{\Phi_{min}}$$

Optimal algorithm to obtain exposures

. . .

$$\xi(n,T) = \int_{\Gamma_{min}}^{\Phi_{min}} |h'_{des} - h'|^p \omega d\Phi + \int_{\Phi_{max}}^{\Gamma_{max}} |h'_{des} - h'|^p \omega d\Phi \qquad \omega = \begin{cases} 0 & h'_{des}(\Phi) < h'(\Phi) \\ 1 & otherwise, \end{cases}$$

Error Function

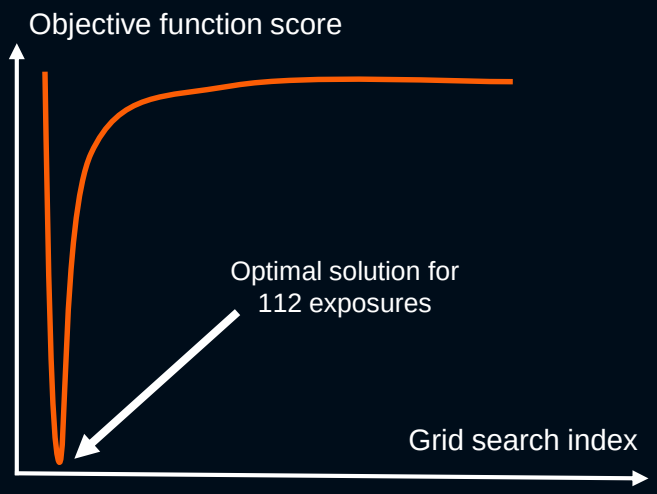
Binary Weights

$$argmin_{n,T} \ \xi(n,T) \ s.t.$$

1. $T_i > 0$
2. $\forall T_i \left[T_i \geq \frac{\tilde{I}_{max}}{\Phi_{min}} \oplus T_i \leq \frac{\tilde{I}_{min}}{\Phi_{max}} \right]$

Grossberg and Nayar 2003

Optimal algorithm to obtain exposures



HDR Image

- Algorithm assumes a single no capture region
- Brute force search is therefore tractable

HDR Results

Over

Under

Fusion

HDR Results

Over

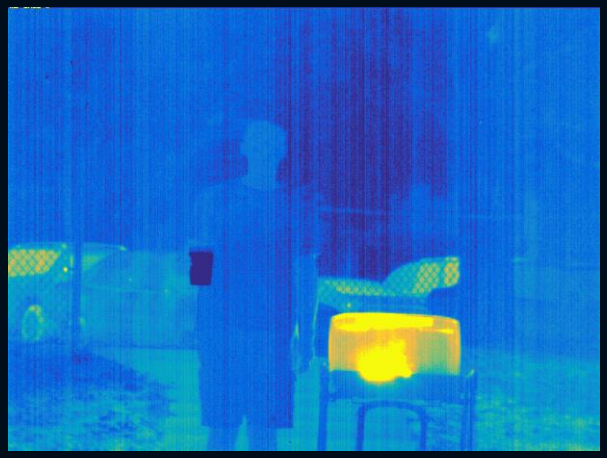
Under

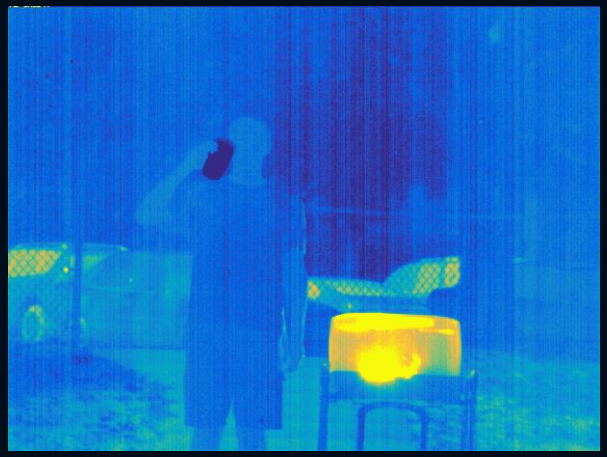
Fusion

HDR Results

Over

Under





Fusion

HDR Results

Method Comparison

Comparison

Digitization

- Low noise
- Good image quality
- Real-time
- Hardware and firmware upgrades

Noise

- Real-time
- No hardware modification
- Low image quality
- Noisy

Exposure

- Low noise
- No hardware modification
- Good image quality
- Multiple Images and more capture time

Future Work

- Pilot deployment program of private sensors at UF Health Shands Hospital.
- Generate database of private face images to for privacy challenge.
- Generate database of private videos for activity recognition in a hospital setting.

Acknowledgements

Sanjeev Koppal

Andreas Enqvist

FLIR

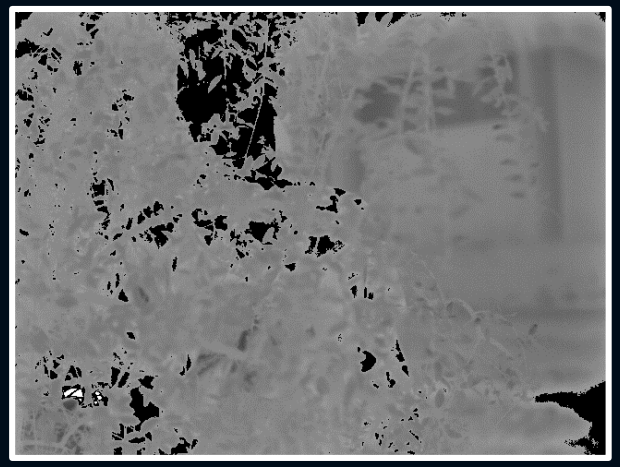
UF | Herbert Wertheim College of Engineering
UNIVERSITY of FLORIDA

DHS

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 2014-DN-077-ARI083-01. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Summary: Three Sensor Level Approaches

Digitization



Noise

Exposure