ReMark: Privacy-Preserving Fiducial Marker System via Single-Pixel Imaging

Tzu-Hsu Yu and Hsin-Mu (Michael) Tsai

Dept. of Computer Science and Information Engineering

National Taiwan University

ACM MobiCom 2023

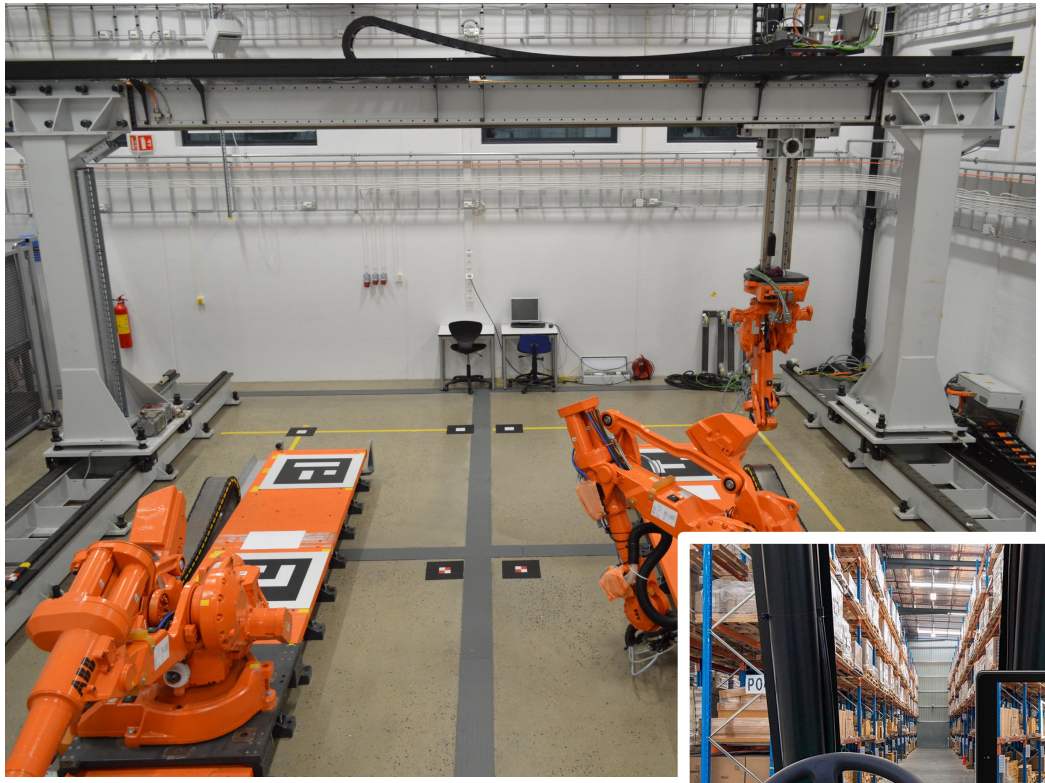
October 5, 2023

國立臺灣大學 National Taiwan University

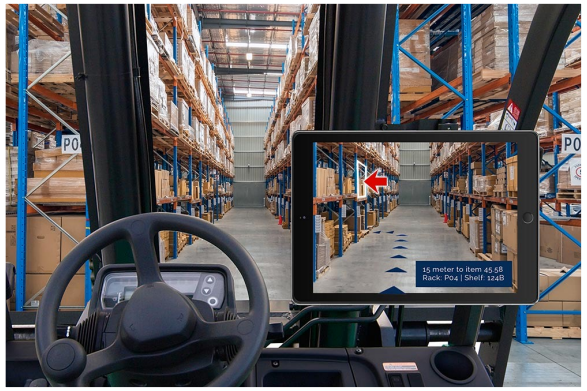
Mobile and Vehicular Network Lab

Fiducial Marker in the Industrial Environments

Indoor Localization and Navigation



https://doi.org/10.3390/s19071561



Img: https://insidernavigation.com

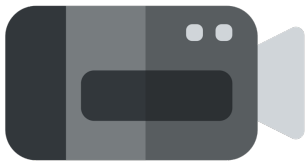
Augmented Reality

Img: https://insidernavigation.com

Markers in the environment or on the objects

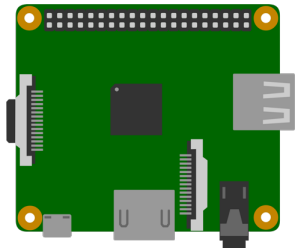
Captured image

Camera sub-system



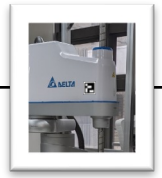
Data bus

(A) Edge device



(C) Network

(B) Cloud server



(A) or (B) perform with :

1. Position and track marker
2. Estimate marker pose
3. Decode marker ID

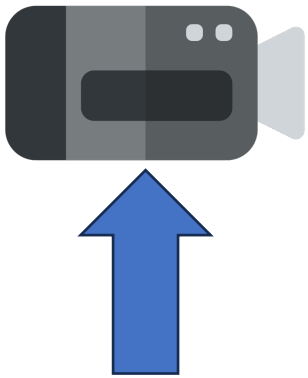
Control commands

Factory scene

Robotic Arm

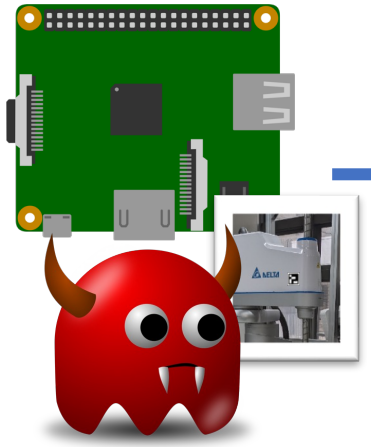
Captured image

Camera sub-system



Data bus

(A) Edge device



(C) Network

(B) Cloud server

Factory scene

Robotic Arm

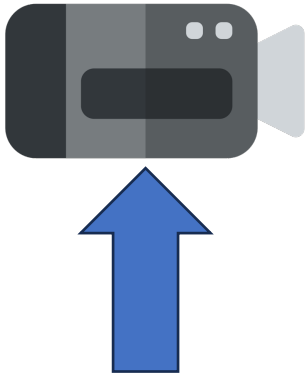
Images can contain private info:

1. Personnel
2. Environment
3. Manufacturing materials and items

Attack!

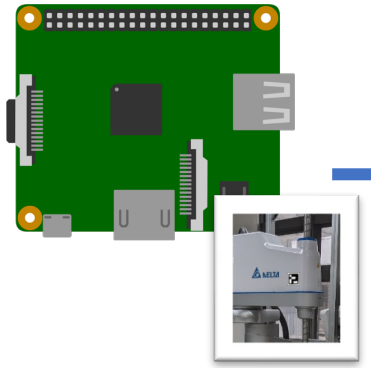
Captured image

Camera sub-system



Data bus

(A) Edge device



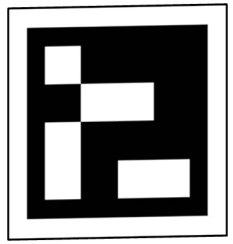
(C) Network

(B) Cloud server

Factory scene

Robotic Arm

Captured image

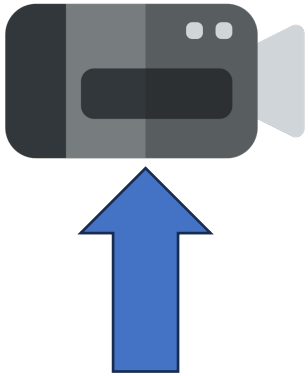


Marker

Background + other objects

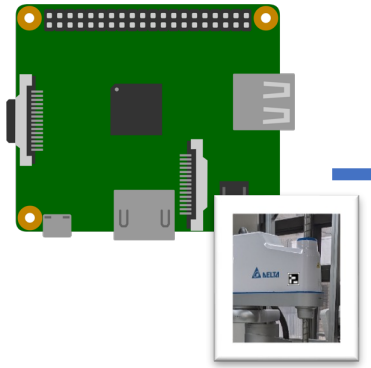
Captured image

Camera sub-system



Data bus

(A) Edge device



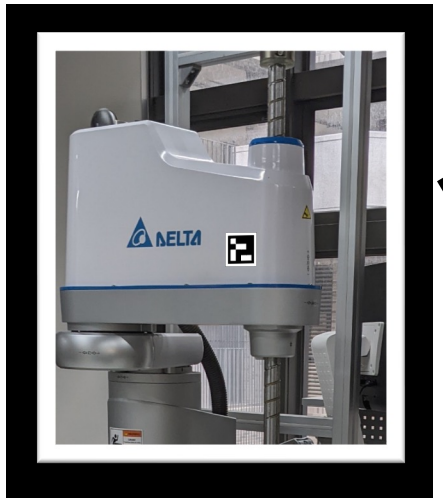
(C) Network

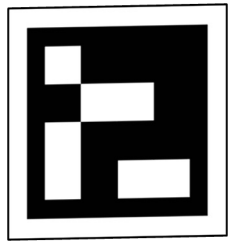
(B) Cloud server

Factory scene

Robotic Arm

Captured image



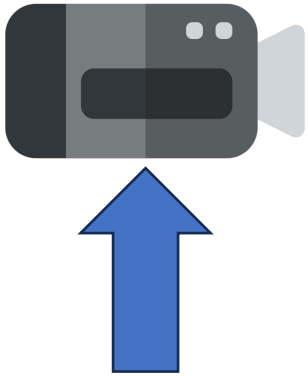


Marker

Background + objects

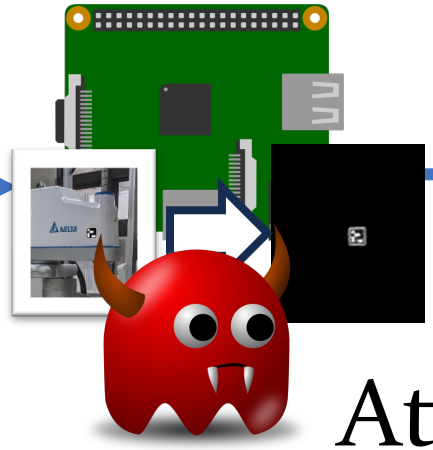
Captured image

Camera sub-system



Data bus

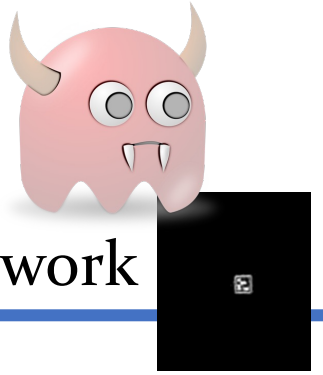
(A) Edge device



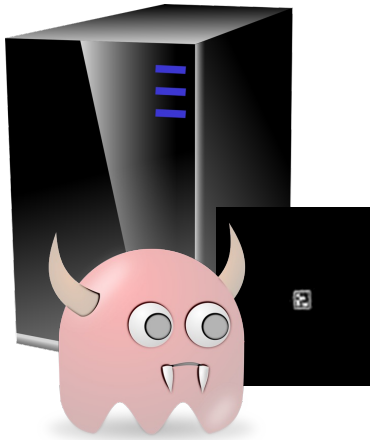
Attack!

Filter out private info here?

(C) Network



(B) Cloud server



Factory scene

Robotic Arm

Idea: Eliminate unnecessary information before it enters the **digital realm**!

Captured image

ReMark

Data bus

(A) Edge device

Network

(B) Cloud server

Nothing
to See Here!

Eliminate
unnecessary info

Digital realm

Physical realm

Factory
scene

Robotic
Arm

Key ideas:
Single-Pixel Imaging + Retroreflector

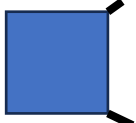
Key ideas:
Single-Pixel Imaging + Retroreflector

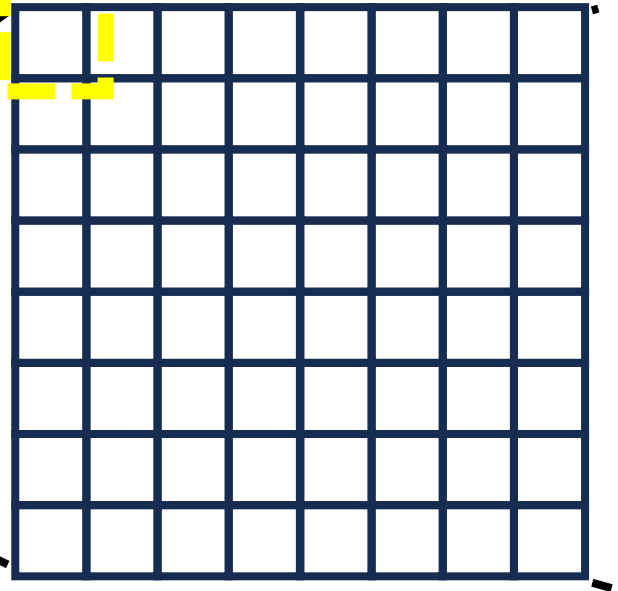
Frequency filtering

Spatial Light Modulator (SLM)

Observed Field of View

Photodiode (light sensor)

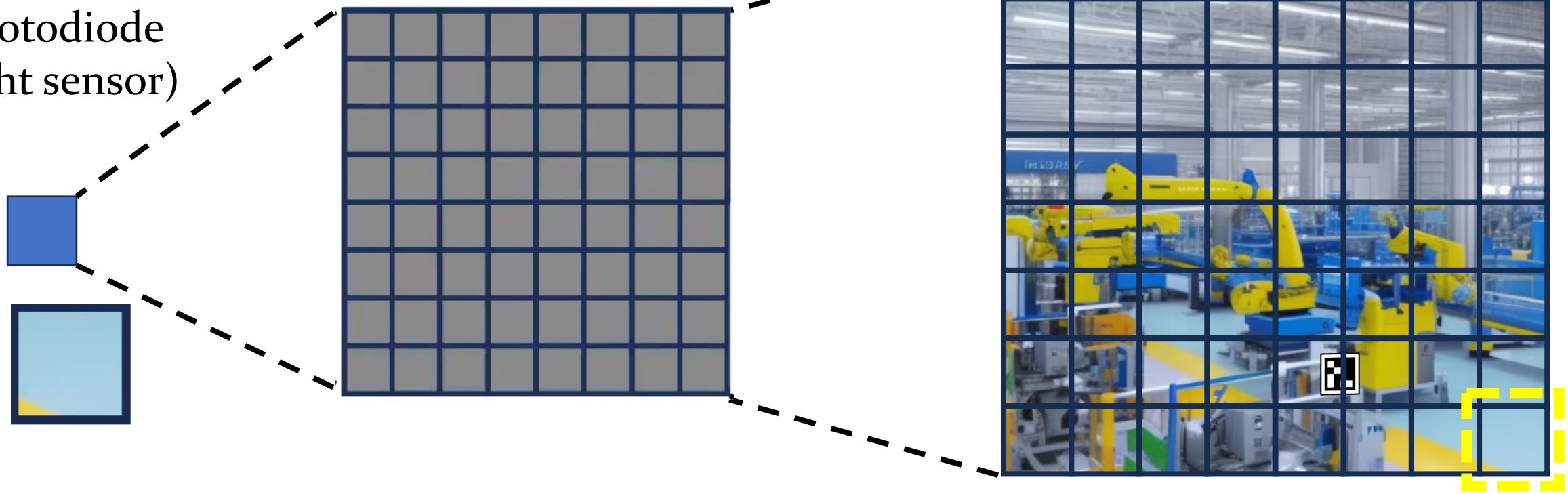




Spatial Light Modulator (SLM)

Observed scene

Photodiode (light sensor)



Naïve Method:
Sequential Observations

Spatial Light Modulator (SLM)

Observed scene

Photodiode (light sensor)

One observation

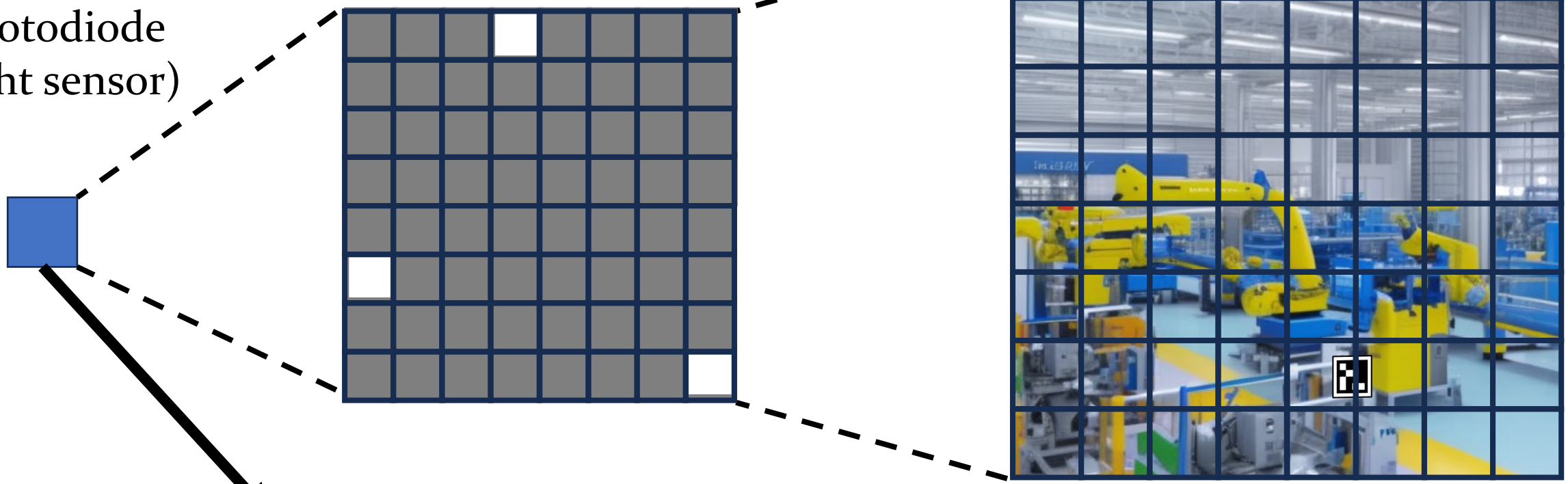
1. One observation captures the sum of multiple pixels.
2. Good observation masks enables accurate estimation of the scene with **less no. of masks**
3. Enumerated, random, or train a neural network!

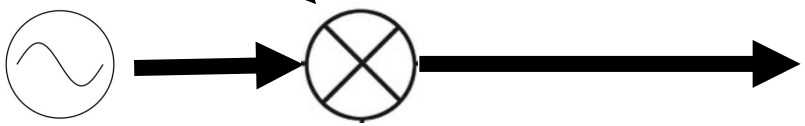
N=No. of SLM pixels
M=No. of masks
Compression Ratio= M/N

Spatial Light Modulator (SLM)

Observed scene

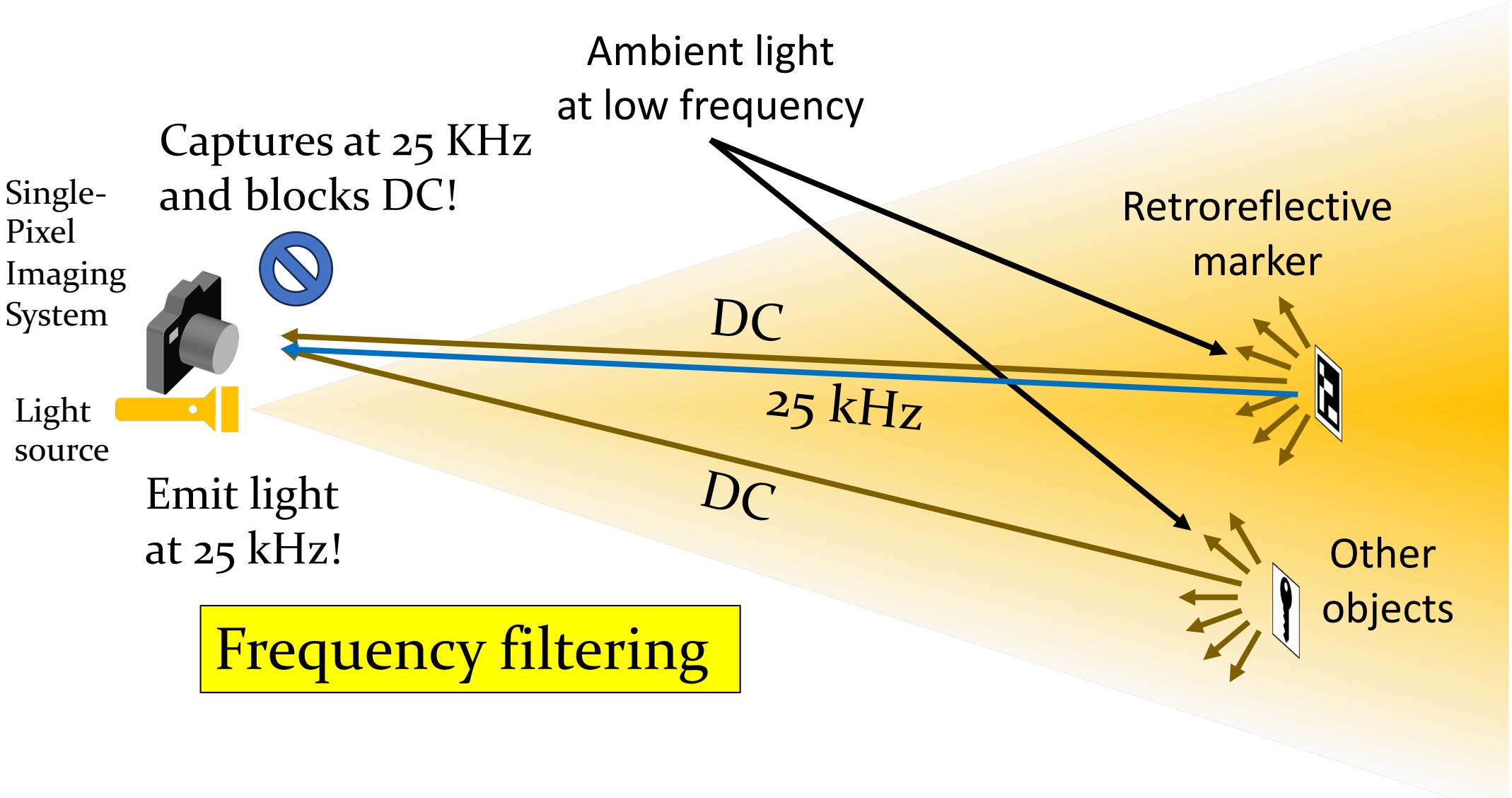
Photodiode (light sensor)





25 KHz Carrier Wave

Capture images at frequency of **25 kHz!**

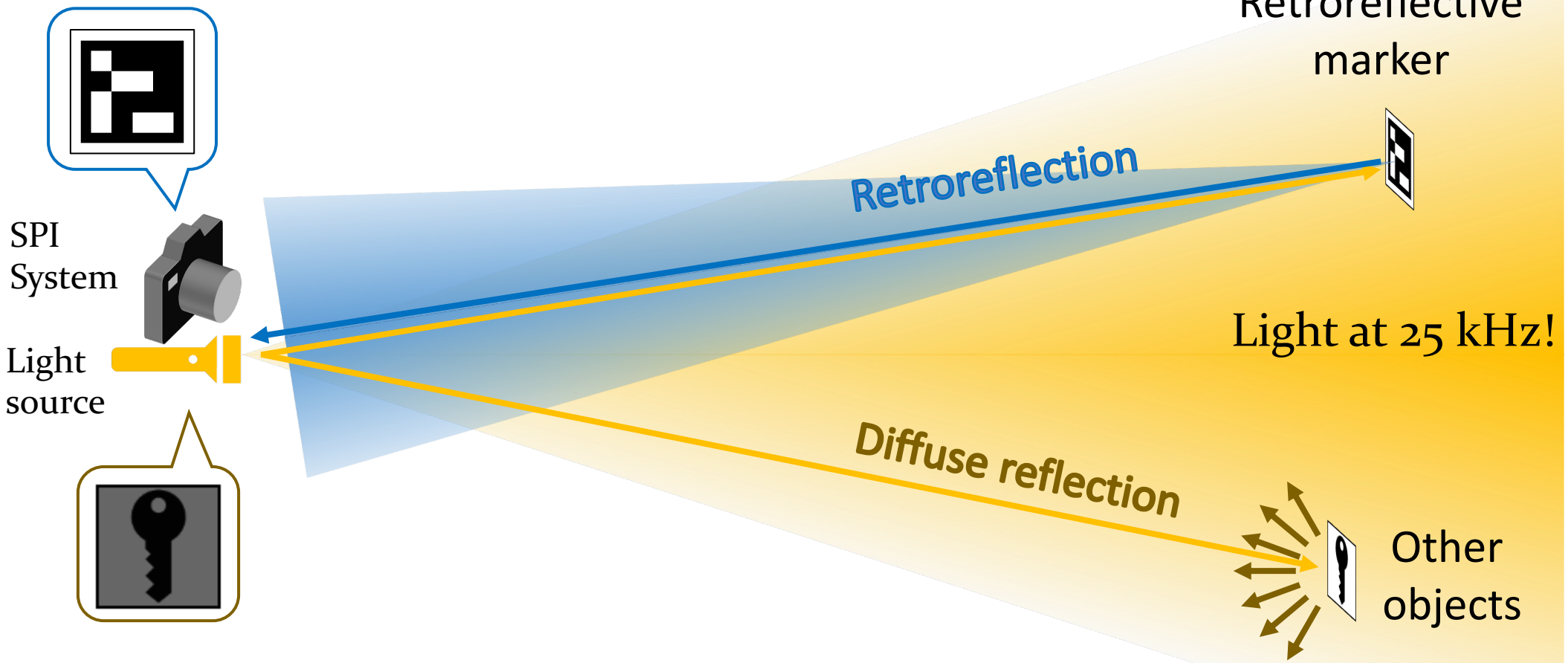


Frequency filtering

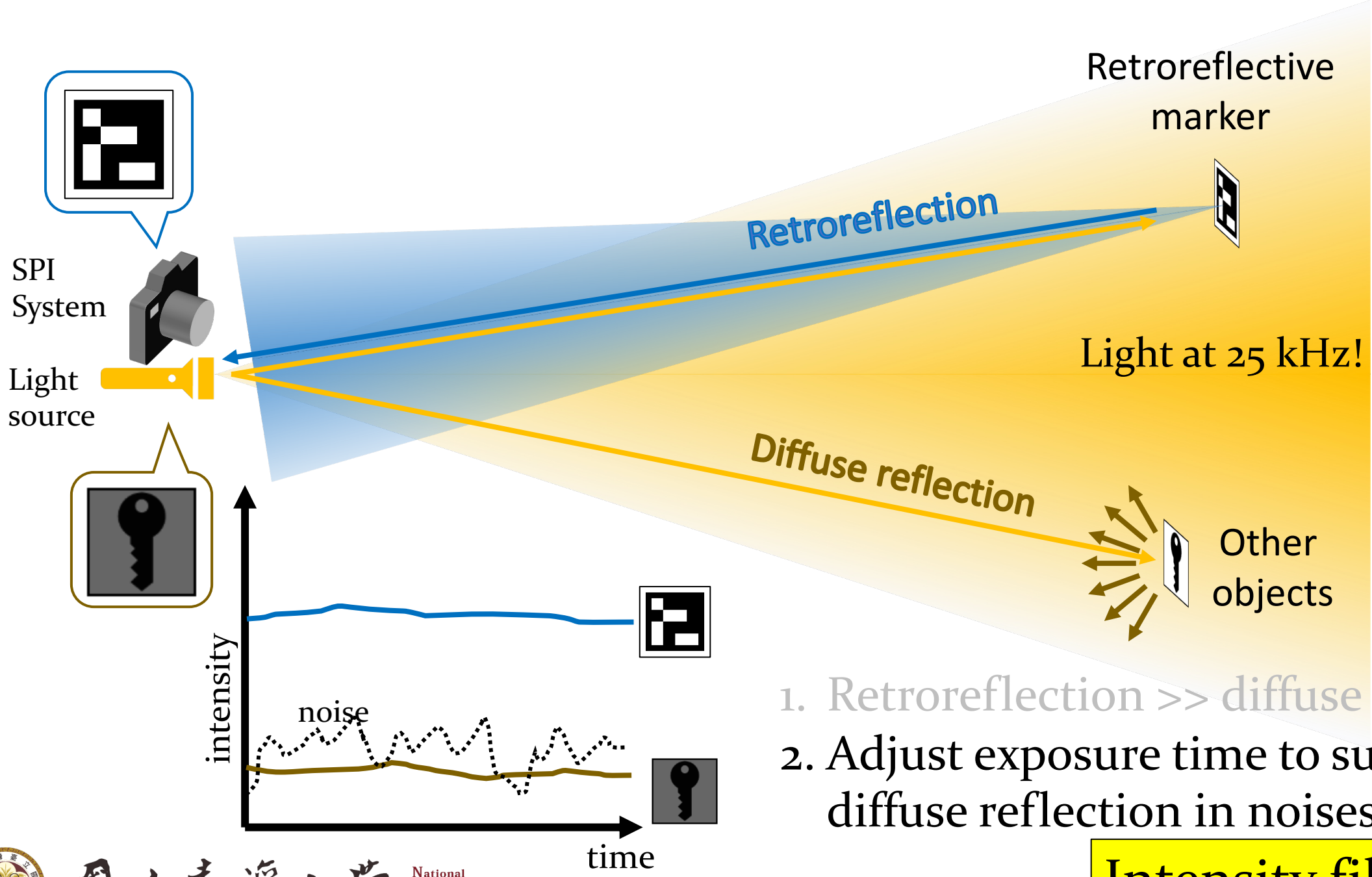
Ordinary light source and ambient light has most energy at DC & low frequency

Key ideas:
Single-Pixel Imaging + Retroreflector

Intensity filtering



1. Retroreflection >> diffuse reflection



1. Retroreflection >> diffuse reflection
2. Adjust exposure time to submerge the diffuse reflection in noises

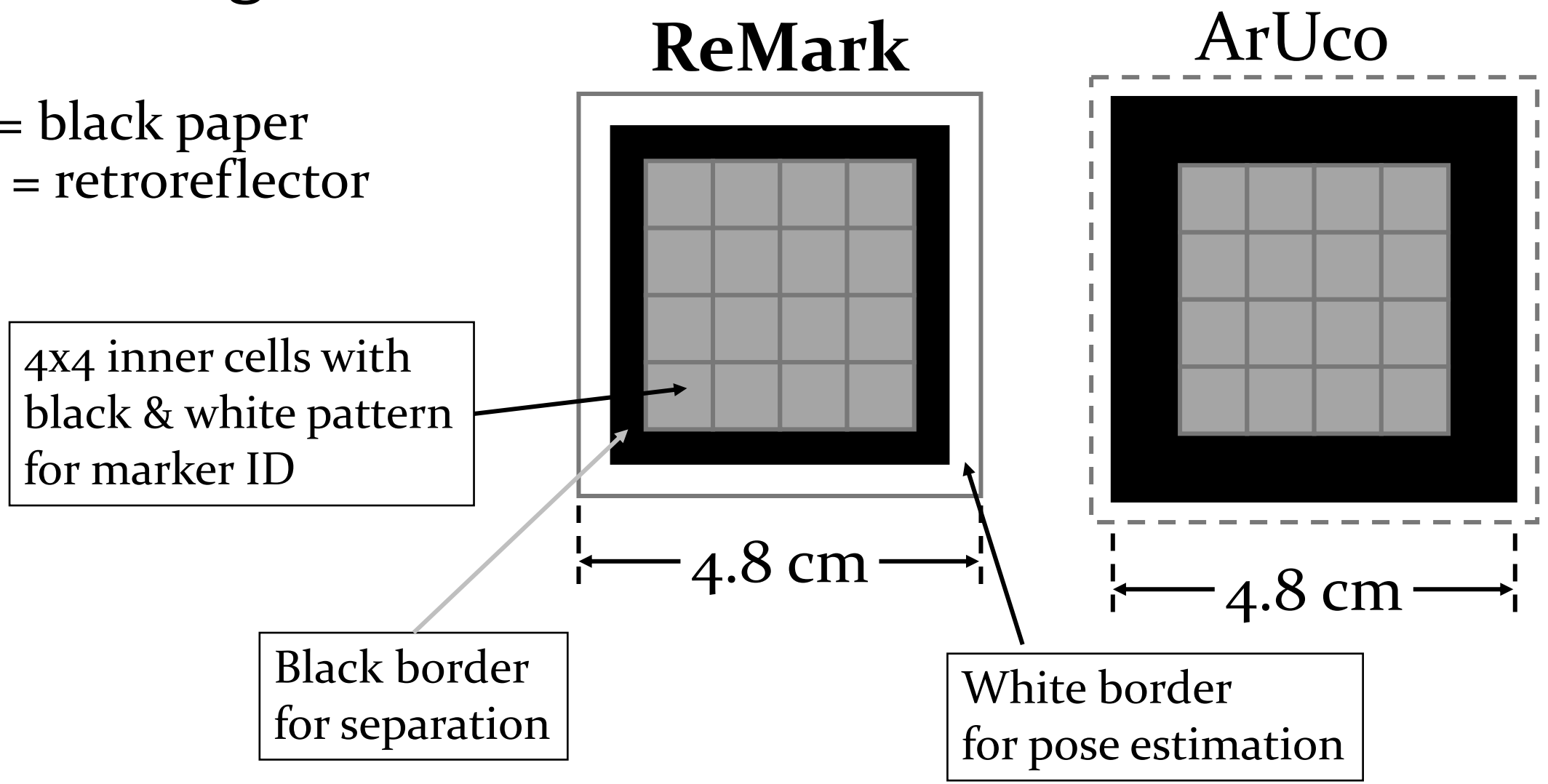
Intensity filtering

System Design

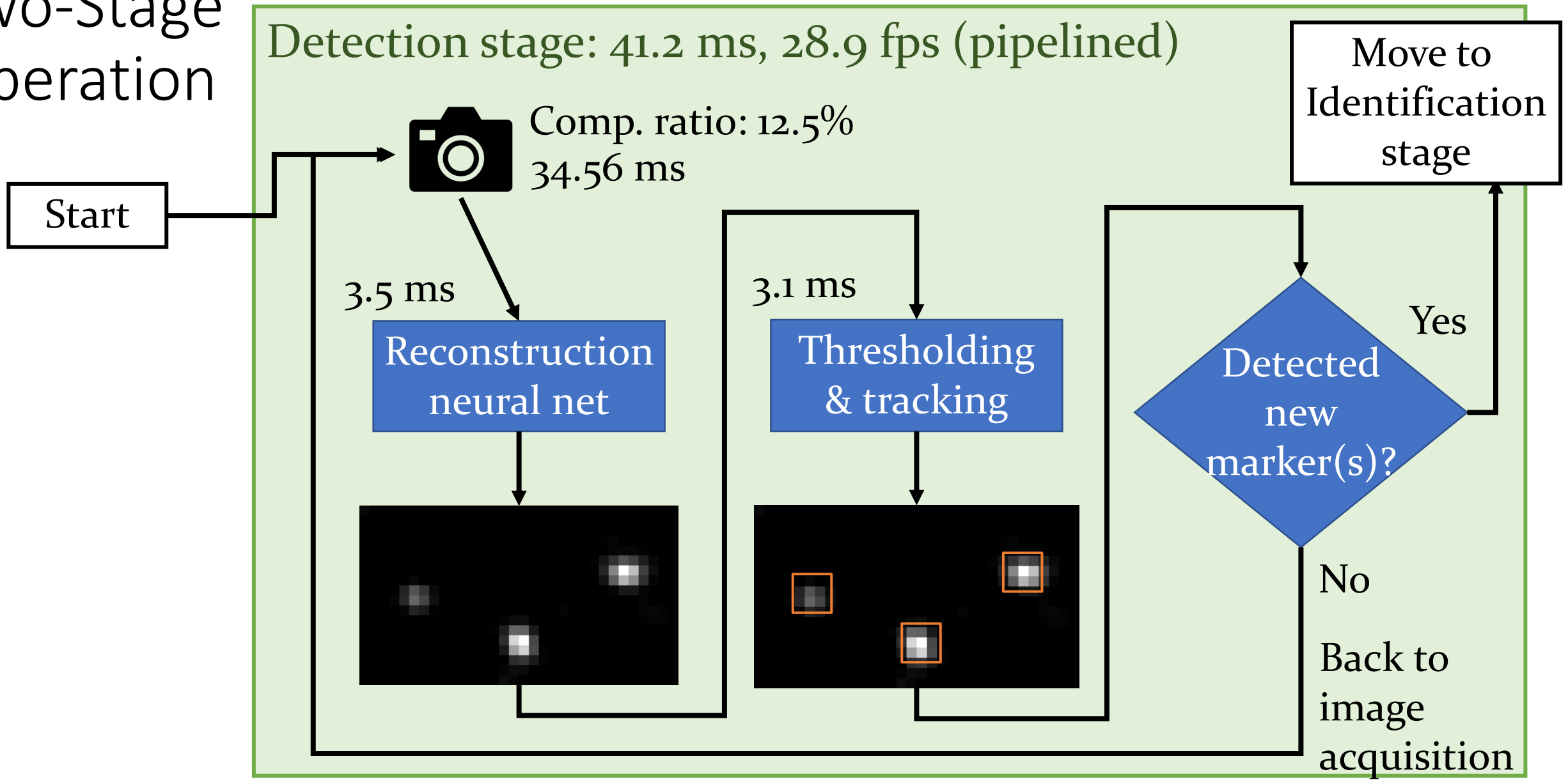
- Overview
  - Key ideas
  - Marker design
  - Two-stage operation
- Challenge 1: Singularity-free embedding for alignment NN
- Challenge 2: Reliable decoding in challenging bias

Marker design

- Black = black paper
  White = retroreflector



Two-Stage Operation



Latencies evaluated with Jetson Nano 2GB

Two-Stage Operation

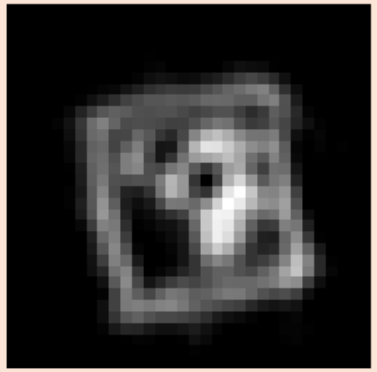
Identification stage: 213.6 ms per new marker

From detection stage

Comp. ratio: 25%
184.32 ms

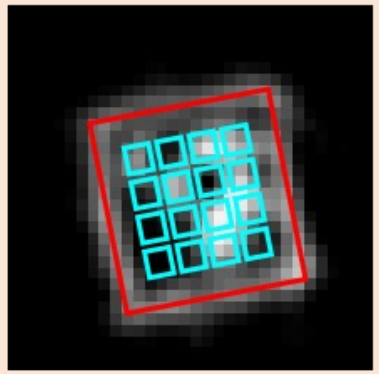
3.5 ms

Reconstruction neural network



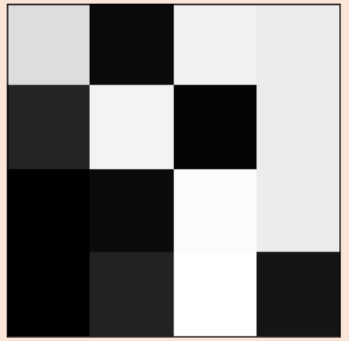
4.1 ms

Alignment neural network



19.5 ms

Extract cells



2.2 ms

Search in dictionary

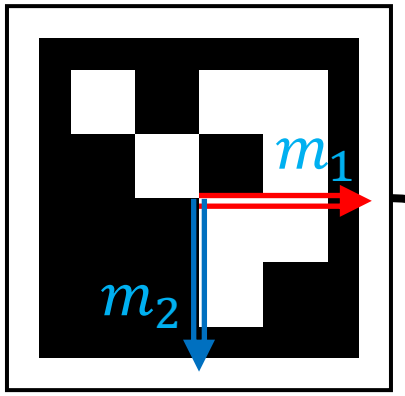
Back to detection stage

System Design

- Overview
  - Key ideas
  - Marker design
  - Two-stage operation
- Challenge 1: Singularity-free embedding for alignment NN
- Challenge 2: Reliable decoding in challenging bias

Alignment Neural Network

- In identification stage
- Estimate the marker pose
- Accurate estimation is crucial to correctly capture the inner cells



Marker coordinate system

Affine transform

$$\begin{bmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{bmatrix}$$

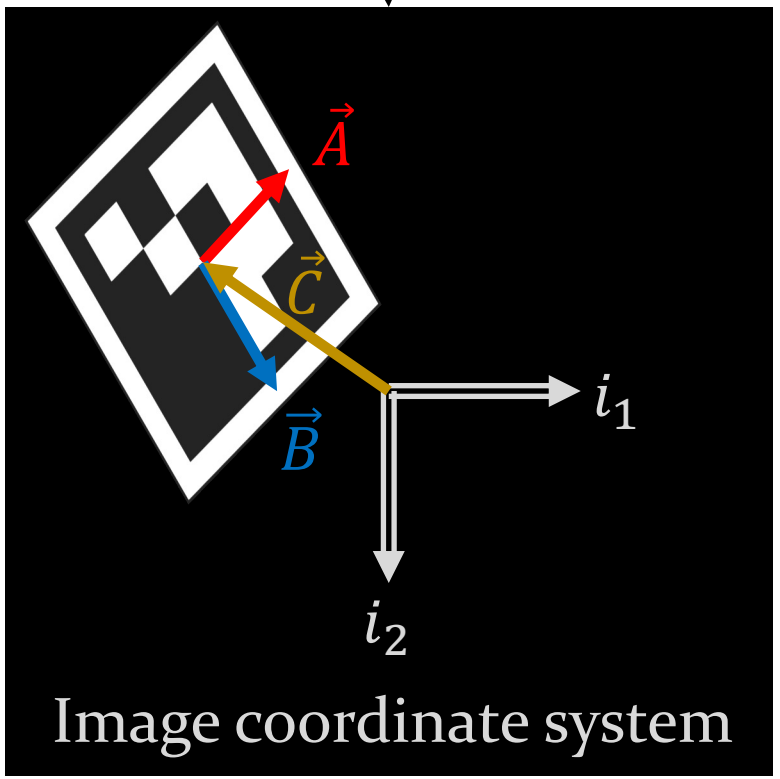
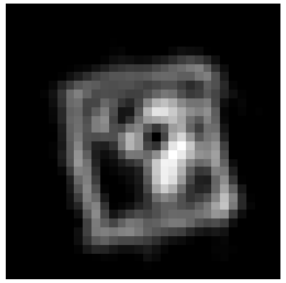


Image coordinate system

Reconstructed image



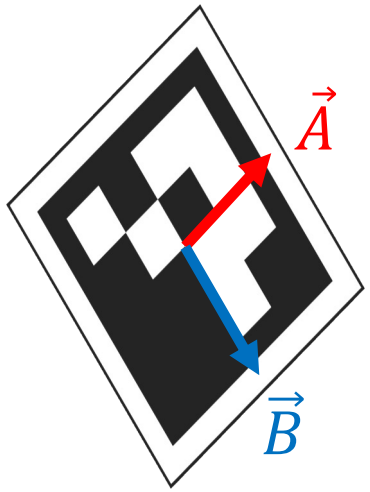
Alignment neural network

Embedding representing marker pose

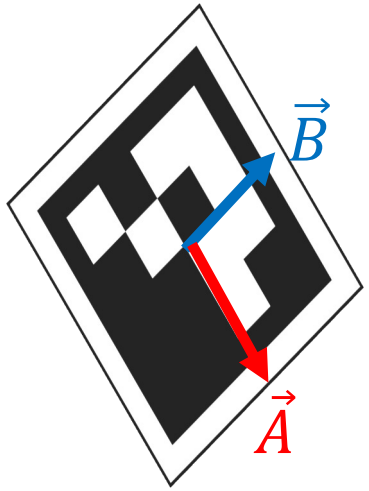
$$\begin{bmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{bmatrix}$$

Singularity-Free Embedding

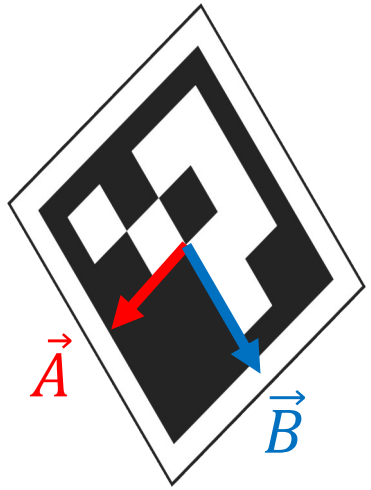
Original



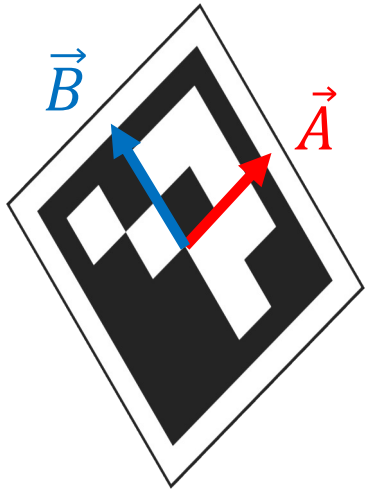
Exchange $\vec{A}$ and $\vec{B}$



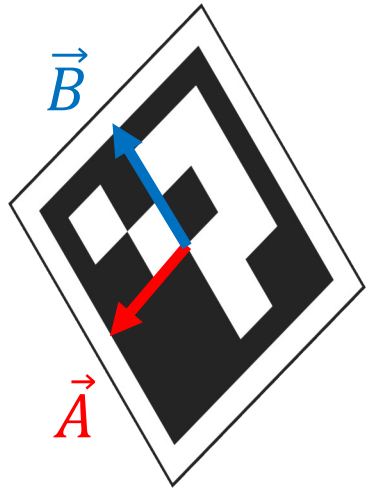
Rotate $\vec{A}$ by 180°



Rotate $\vec{B}$ by 180°



Rotate both by 180°



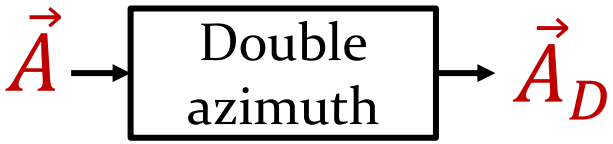
- Same parallelogram, different values of $\vec{A}$ and $\vec{B}$ in the output
  → violating **one-to-one correspondence**
- Imposing restrictions on the values of $\vec{A}$ and $\vec{B}$
  → loss of **continuity**

Restrictions:

$$(1)\ \angle\vec{A},\ \angle\vec{B} \in [-90°, 90°)$$

$$(2)\ \angle\vec{A} - \angle\vec{B} \in [0°, 180°)$$

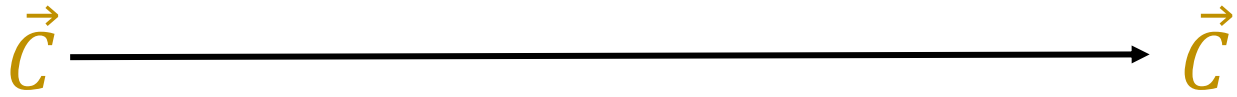
Singularity-Free Embedding



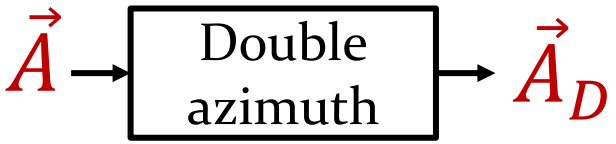
$$\vec{A} = (a\cos\theta\,, a\sin\theta)$$

$$\overrightarrow{A_D} = (a\cos 2\theta\,, a\sin 2\theta)$$

$\vec{B}$ $\vec{B}_D$



Singularity-Free Embedding



$\vec{B}$ $\vec{B}_D$

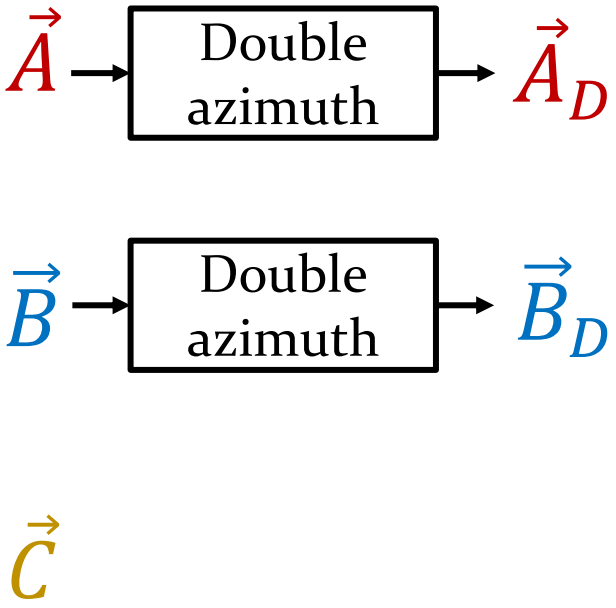
$\vec{C}$

$$\vec{A} = (a\cos\theta\,, a\sin\theta)$$

$$\overrightarrow{A_D} = (a\cos 2\theta\,, a\sin 2\theta)$$

Rotate $\vec{A}$ by 180° produce the same $\overrightarrow{A_D}$!

Singularity-Free Embedding



$$\vec{A} = (a\cos\theta\,, a\sin\theta)$$

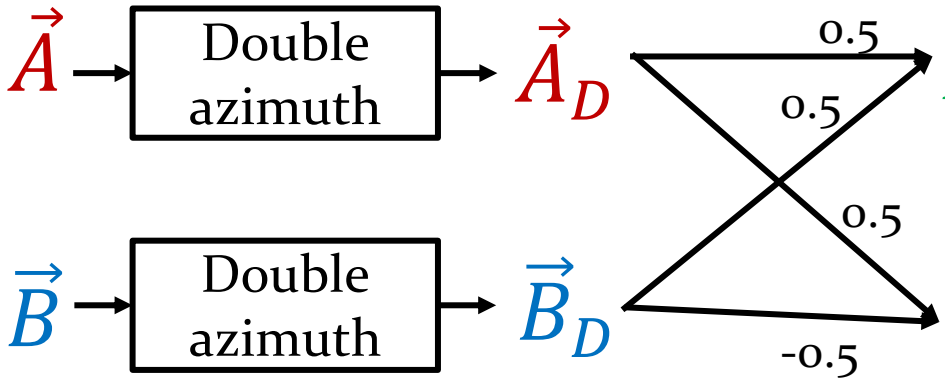
$$\overrightarrow{A_D} = (a\cos 2\theta\,, a\sin 2\theta)$$

Rotate $\vec{A}$ by 180° produce the same $\overrightarrow{A_D}$!

Rotate $\vec{B}$ by 180° produce the same $\overrightarrow{B_D}$!

Singularity-Free Embedding

Exchange $\vec{A}$ and $\vec{B}$ produces the same $\vec{M}$



$$\vec{M} = \frac{1}{2}(\vec{A}_D + \vec{B}_D)$$

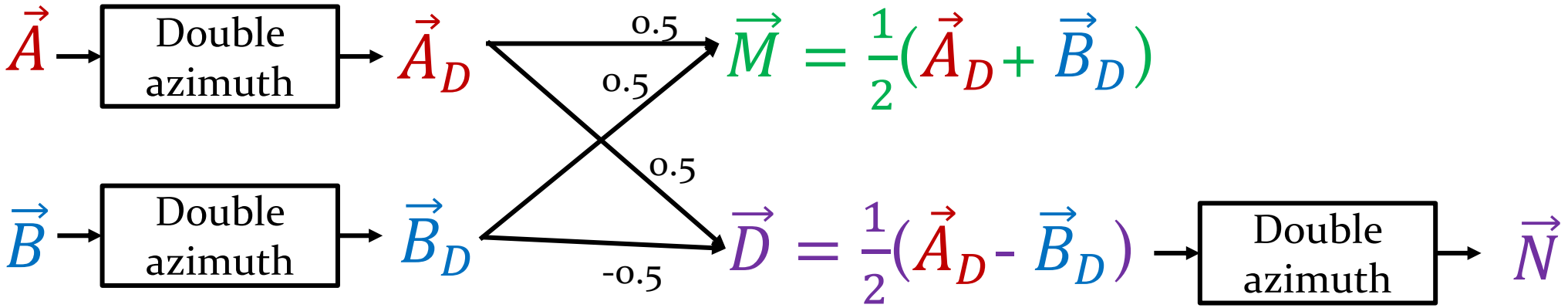
$$\vec{D} = \frac{1}{2}(\vec{A}_D - \vec{B}_D)$$

$\vec{C}$

Exchange $\vec{A}$ and $\vec{B}$ produces $-\vec{D}$ (rotate by 180°)

Singularity-Free Embedding

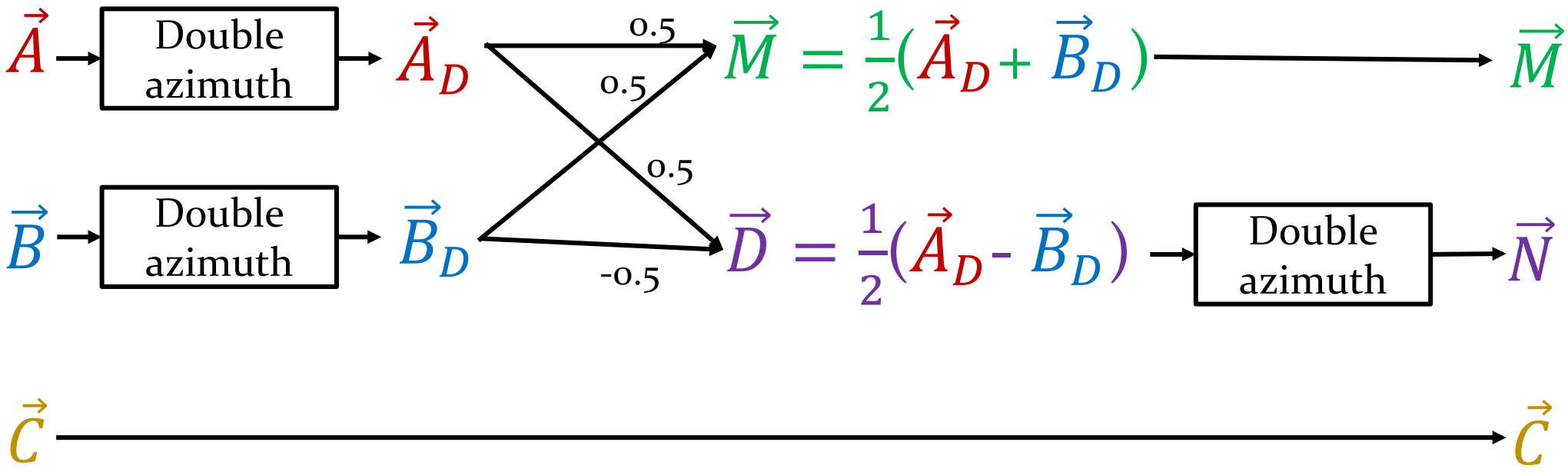
Exchange $\vec{A}$ and $\vec{B}$ produces the same $\vec{M}$



$\vec{C}$

Exchange $\vec{A}$ and $\vec{B}$ produces the same $\vec{N}$

Singularity-Free Embedding



Alignment NN embedding

$$\begin{bmatrix} M_1 & N_1 & C_1 \\ M_2 & N_2 & C_2 \end{bmatrix}$$

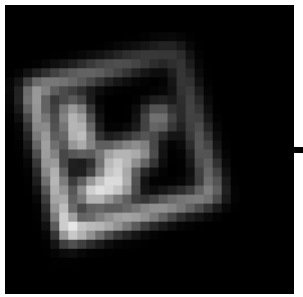
Singularity-free!

System Design

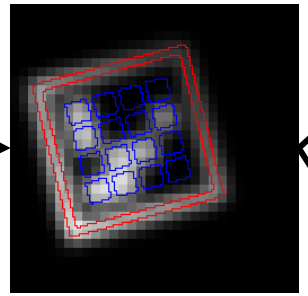
- Overview
  - Key ideas
  - Marker design
  - Two-stage operation
- Challenge 1: Singularity-free embedding for alignment NN
- Challenge 2: Reliable decoding in strong bias

Soft-Decision Decoding

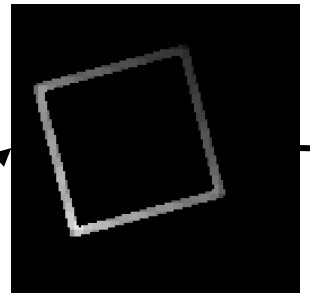
Please take a look at our paper!



Subdivide macropixels

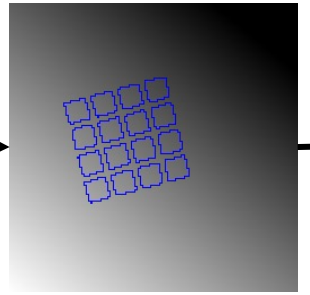


Crop



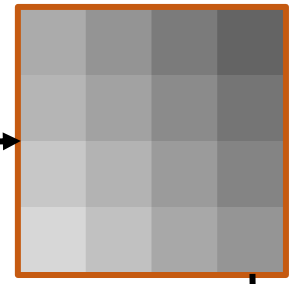
White border

Fit to linear function



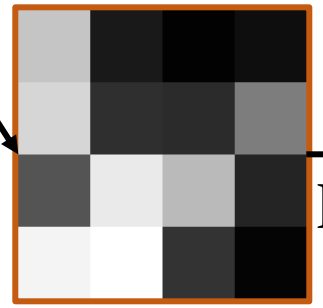
Bias function

Crop & sum

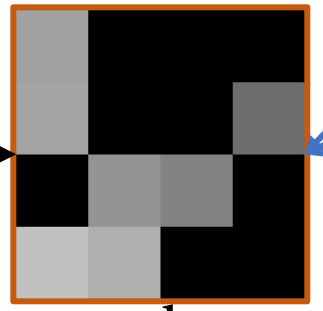


Estimated bias B

Crop & sum

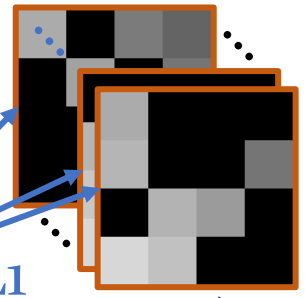


Deblur



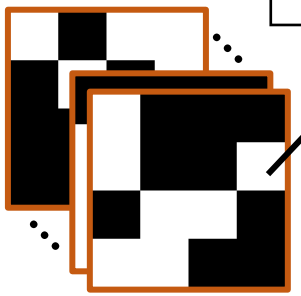
Extracted cells I

L1 distance



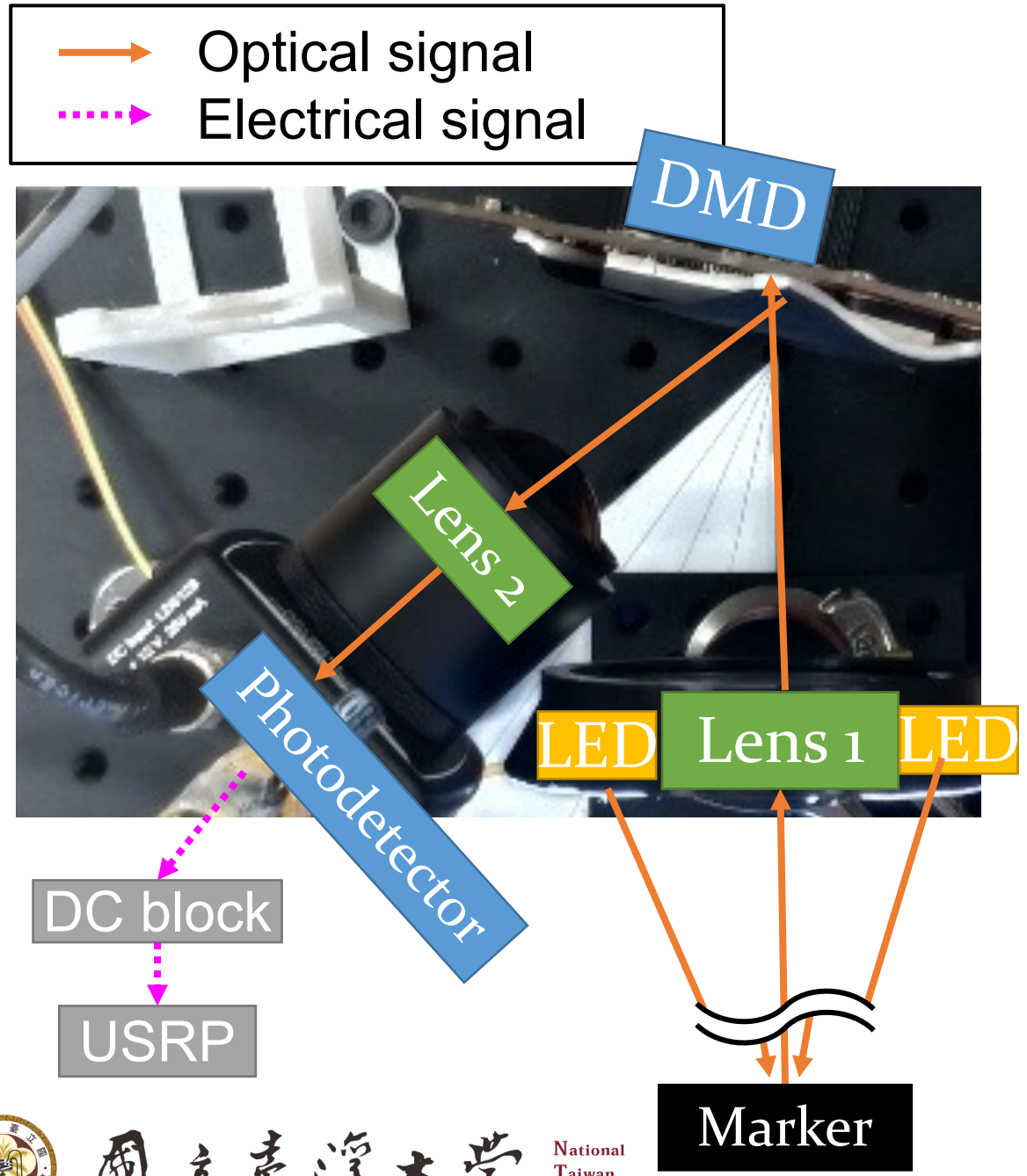
Multiply

Dictionary D^{aug}



Output the marker ID from the dictionary with the **smallest L1 distance**.

Evaluation


Optical signal
Electrical signal
DMD
Lens 2
Photodetector
LED
Lens 1
LED
DC block
USRP
Marker

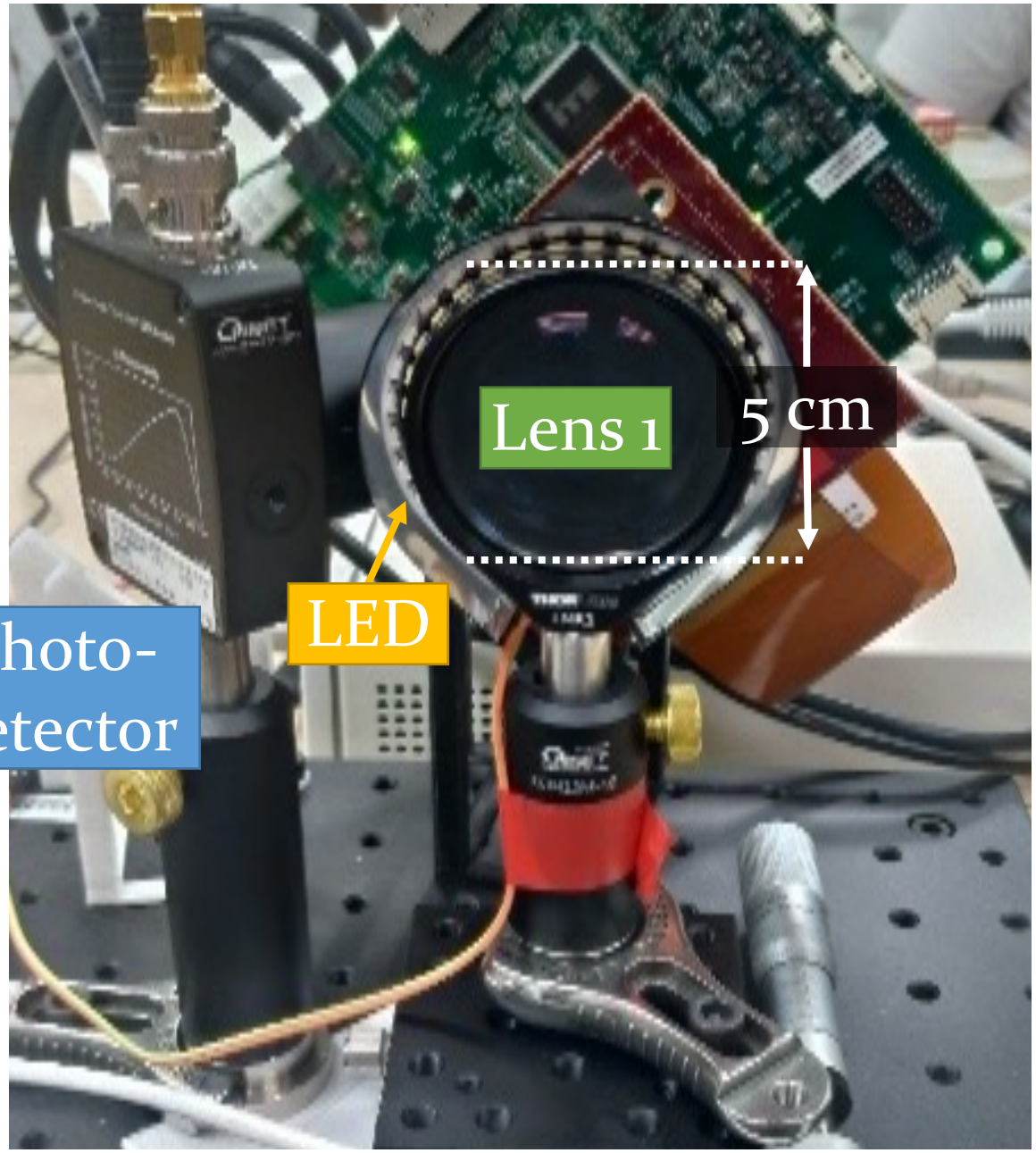


Photo-
detector
LED
Lens 1
5 cm

A Quick Summary of Results

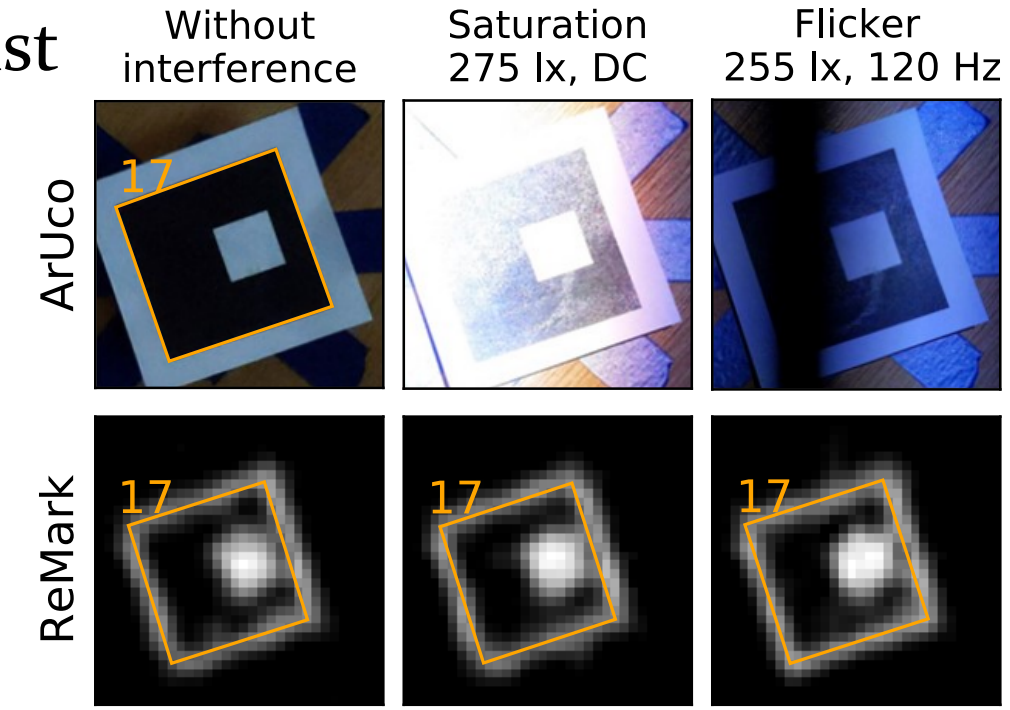
- Detection stage:

Save **29%** of acquisition time	Save **73%** of reconstruction time	Support **200 cm/s** mobility	**28.9 fps** detection frame rate	**99.3%** detection rate (1 marker)

- Identification stage:

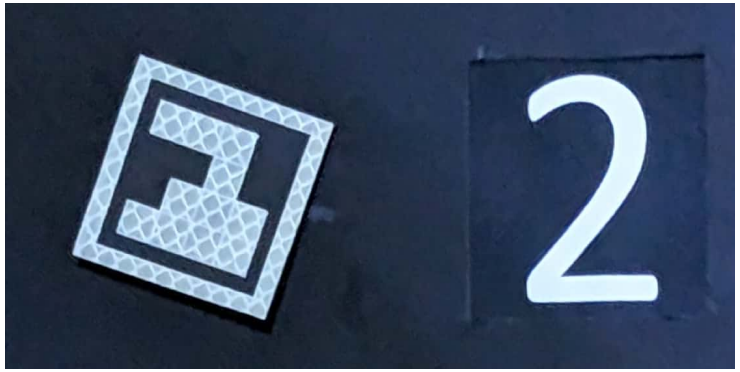
2.1% decode error rate	Soft-decision reduces error by **60%**	
4.7 marker/s identification rate	up to **30°** tilt angle	**3-5 m** working distance

Robust against interference:

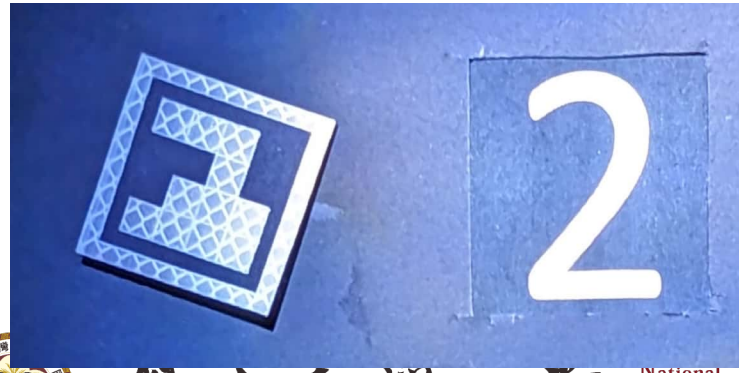


Frequency and Intensity Filtering

Ambient DC illumination:
22 lx

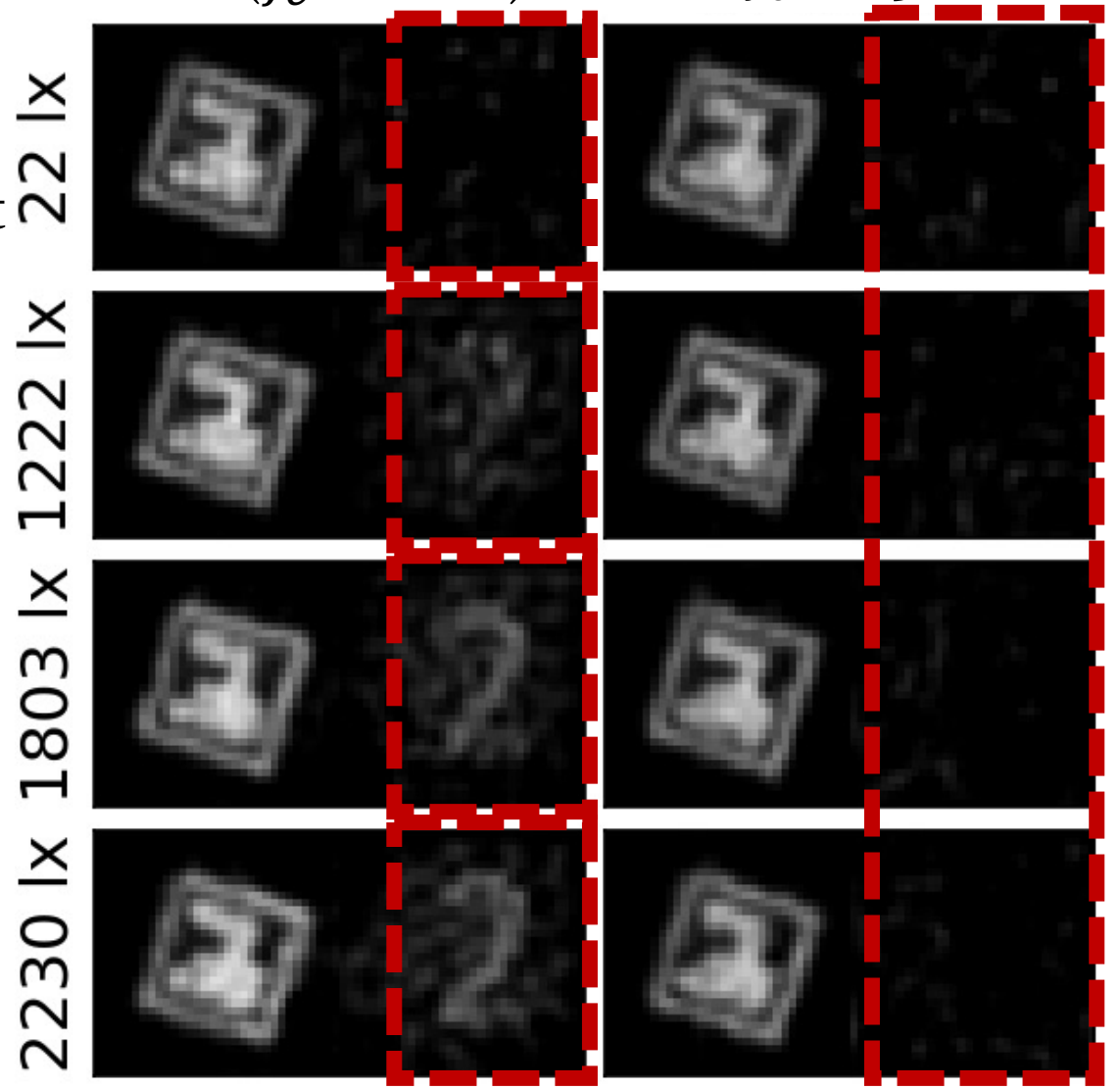


Ambient DC illumination:
2230 lx

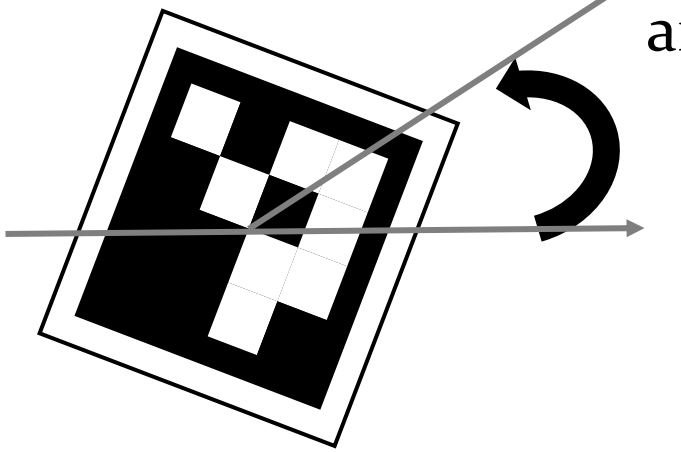


1. Retroreflector returns more light than background objects due to intensity filtering
2. No longer work with more ambient illumination
3. No effect for ReMark operating at 25 kHz!

Intensity filtering only (Camera + retroref.)	Intensity + freq. filtering (ReMark)



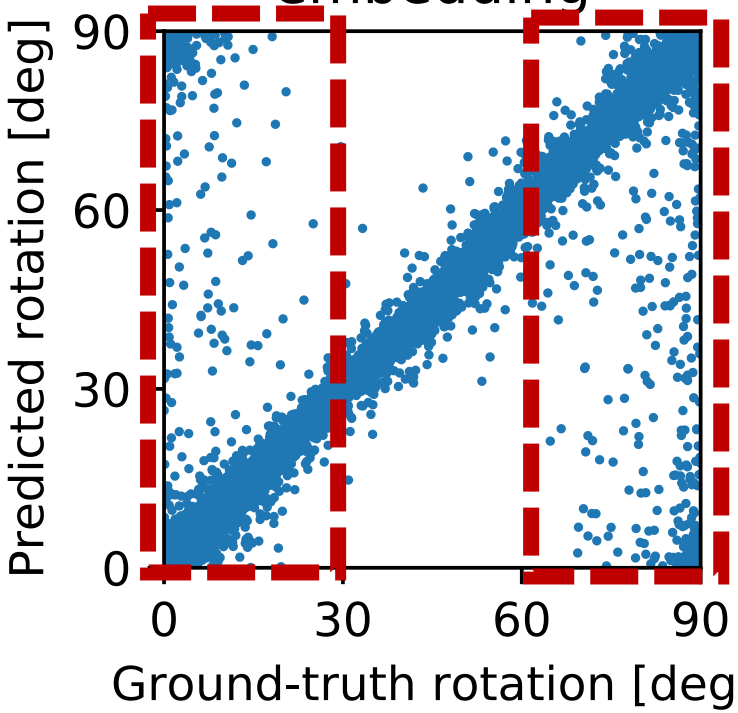
Singularity-Free Embedding for Alignment NN



Eliminate
inaccuracy and outliers!

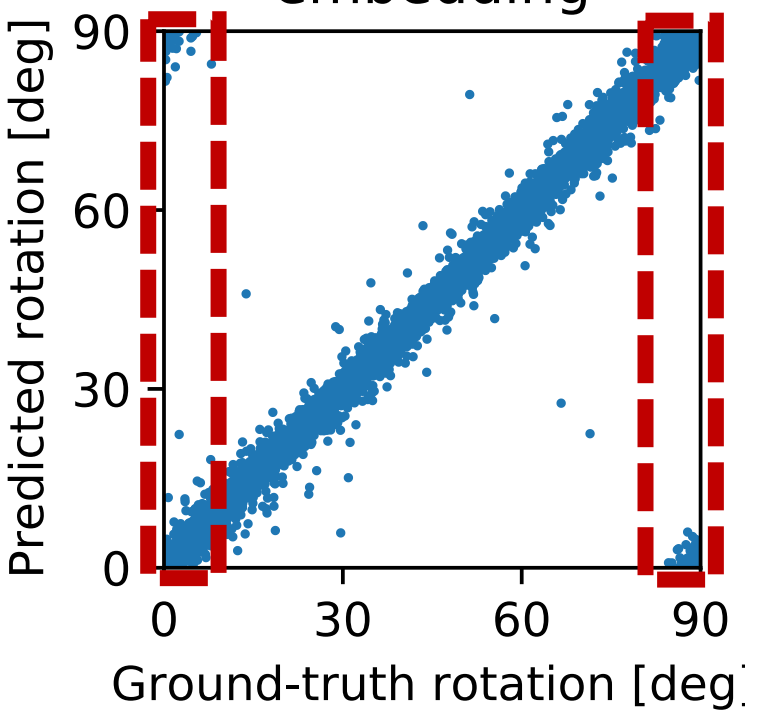
Naïve embedding

Discontinuous
embedding



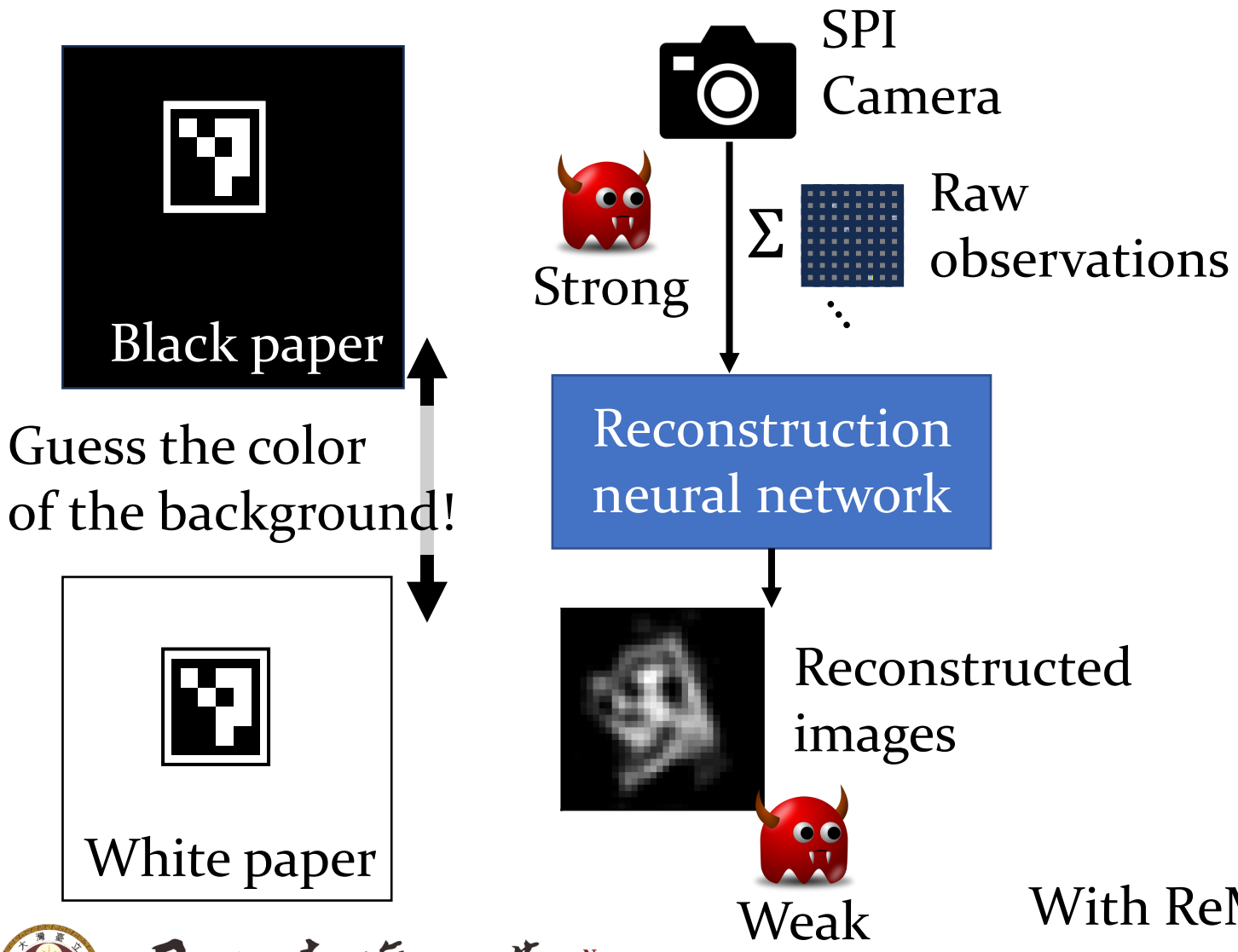
Singularity-free
embedding

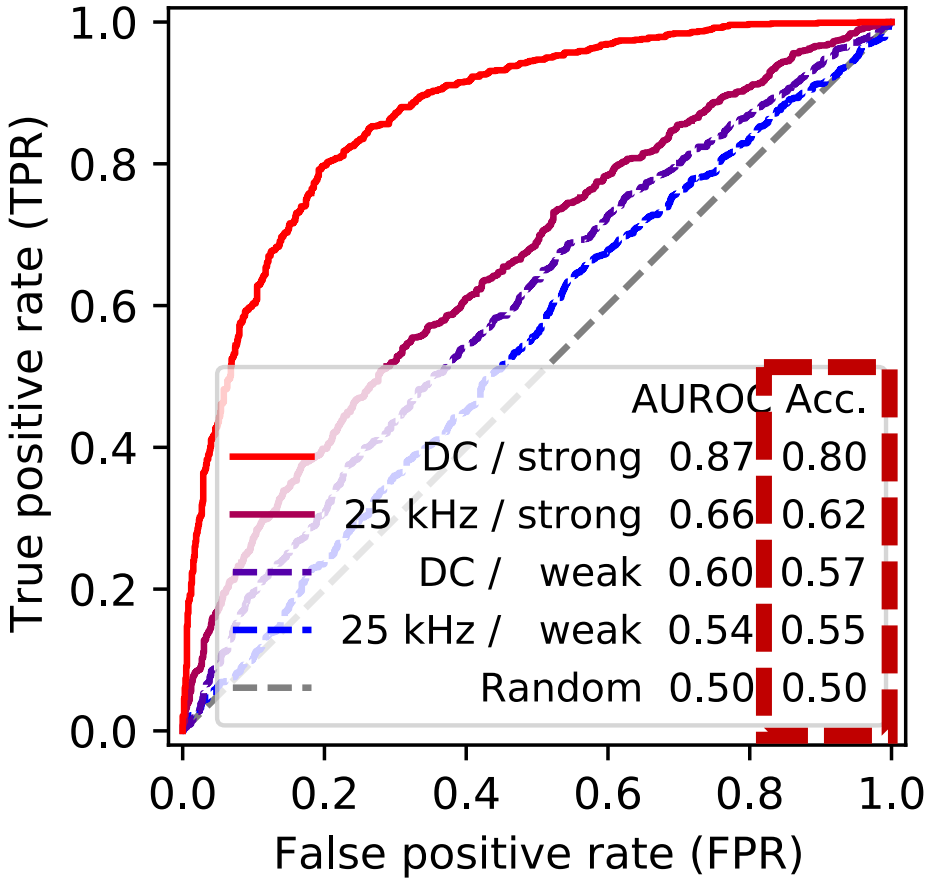
Continuous
embedding



Privacy Preservation

Option 1. DC = Camera + retroref.
Option 2. 25 kHz = ReMark





With ReMark, even guessing 1-bit information is next to random guess!

Conclusion

- Implemented a fiducial marker system (detection + identification) which removes sensitive information before it enters **digital realm**
- Single-pixel imaging (SPI) + retroreflector = **Frequency + intensity filtering**
- Performance numbers:

Detection			Identification	
99% detection rate	28.9 fps detection frame rate	Support 200 cm/s mobility	2.1% decode error rate	4.7 marker/s identification rate

國立臺灣大學 National Taiwan University

ReMark: Privacy-reserving Fiducial Marker System via Single-Pixel Imaging

Tzu-Hsu Yu and **Hsin-Mu (Michael) Tsai**

National Taiwan University

Email: hsinmu@ntu.edu.tw

Find out more about our papers!

國立臺灣大學 National Taiwan University

Mobile and Vehicular Network Lab