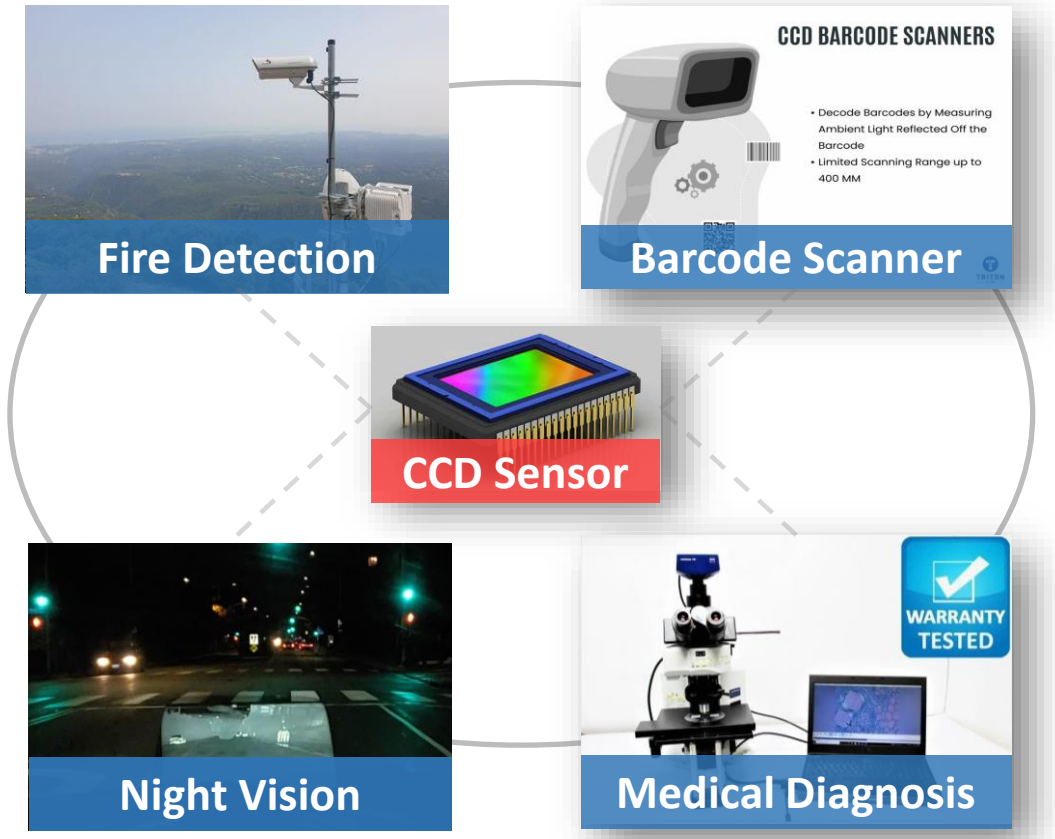
GhostShot: Manipulating the Image of CCD Cameras with Electromagnetic Interference

Yanze Ren, Qinhong Jiang, Chen Yan, Xiaoyu Ji, Wenyuan Xu

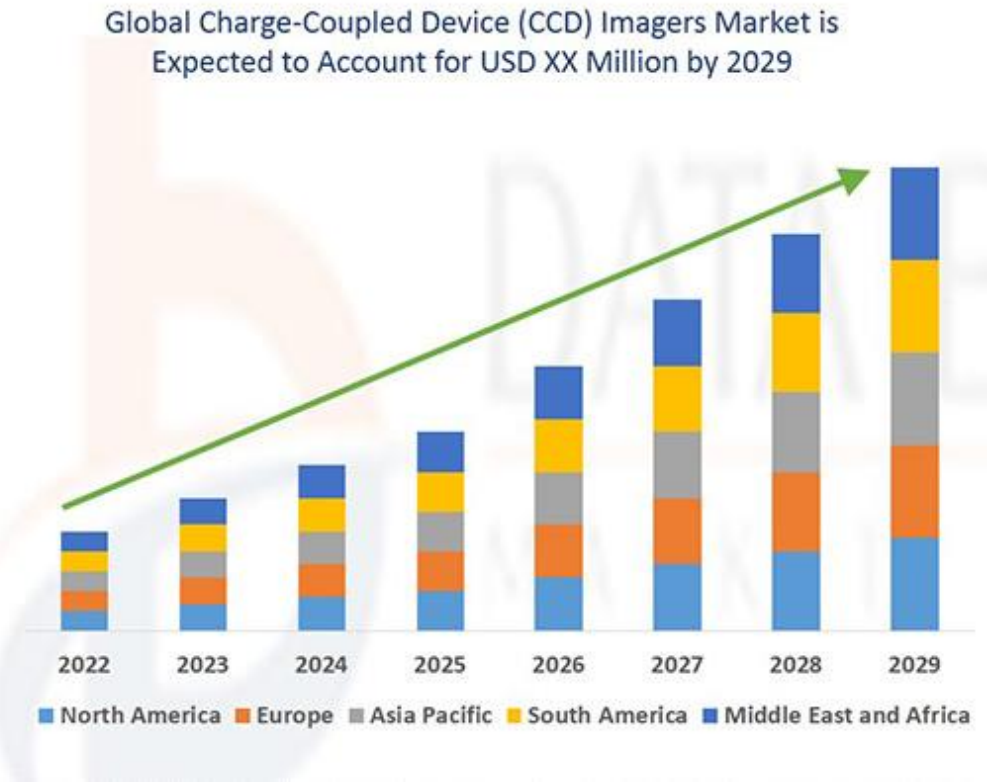
Ubiquitous System Security Lab (USSLAB), Zhejiang University

CCD Cameras

The **CCD (Charge Coupled Device)** is a critical type of camera, and the reliability of the images it captures plays a key role in the decision-making of subsequent intelligent systems.

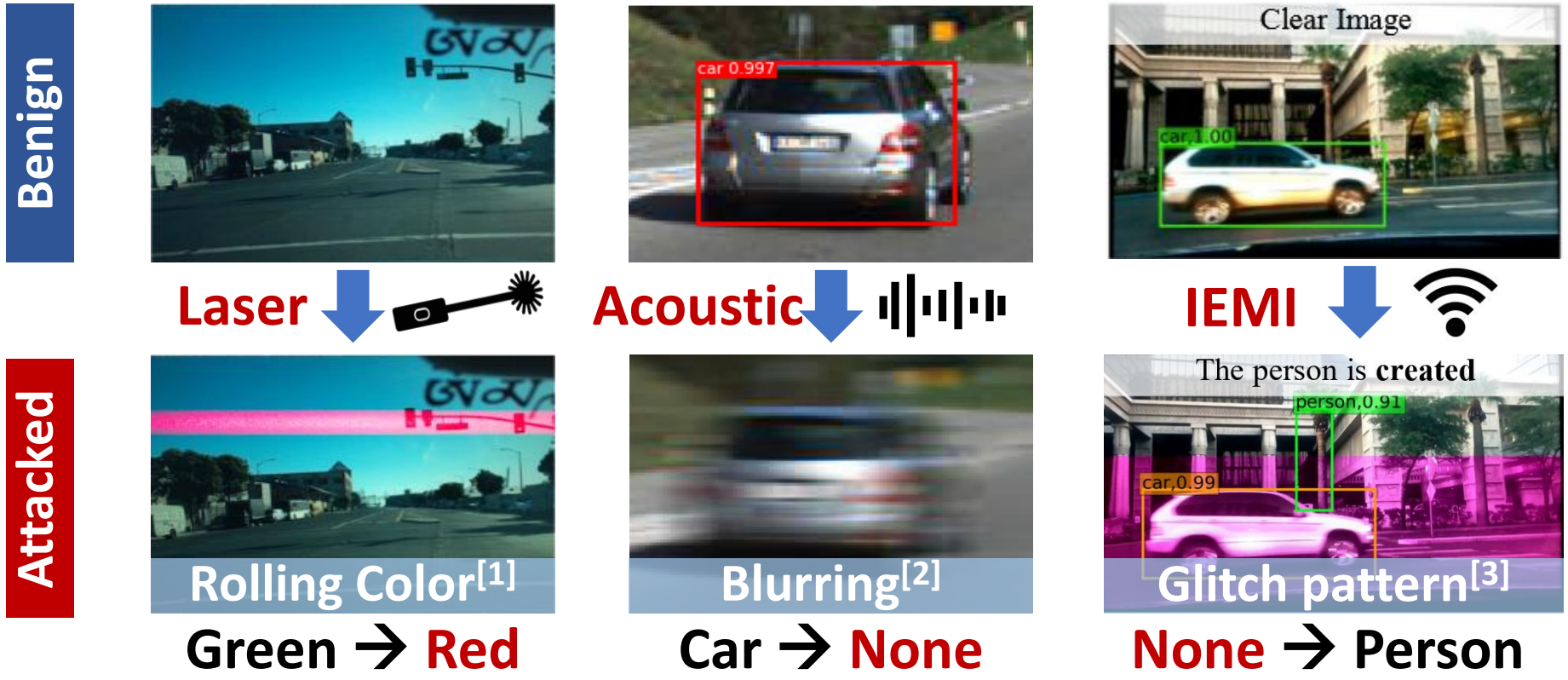


CCD Cameras Application



The growth of CCD market[1]

Previous Attacks on Cameras



Can more **fine-grained** interference be implemented on camera systems?

[1] Yan et al., Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition (USENIX 2022)
[2] Ji et al., Poltergeist: Acoustic Adversarial Machine Learning against Cameras and Computer Vision (S&P 2021)
[3] Jiang et al. GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI (USENIX 23)

Previous Attacks on Cameras

Injection under dark conditions

Injection under normal light conditions

Previous work [1] shown the feasibility of injection into CCD sensors, however:

- **Noticeable image** could only be injected in a **dark environment**
- Injection changes are **unnoticeable under normal light conditions**

[1] S. Kohler et al. Signal Injection Attacks against CCD Image Sensors (ACM ASIACCS 22).

Previous Attacks on Cameras

Injection under dark conditions

Injection under normal light conditions

Previous work has inspired us to consider :

- Is this a **real-world threat** under normal lighting conditions?
- What are **the limits of** the attack's capability and the **potential harm**?

[1] S. Kohler et al. Signal Injection Attacks against CCD Image Sensors (ACM ASIACCS 22).

Can we inject arbitrary colorful patterns in any ambient light conditions into the image captured by CCD cameras?

For Example

Adversary

IEMI

CCD Camera

Night Vision Detection

QR code scanning

Fire detection

For Example

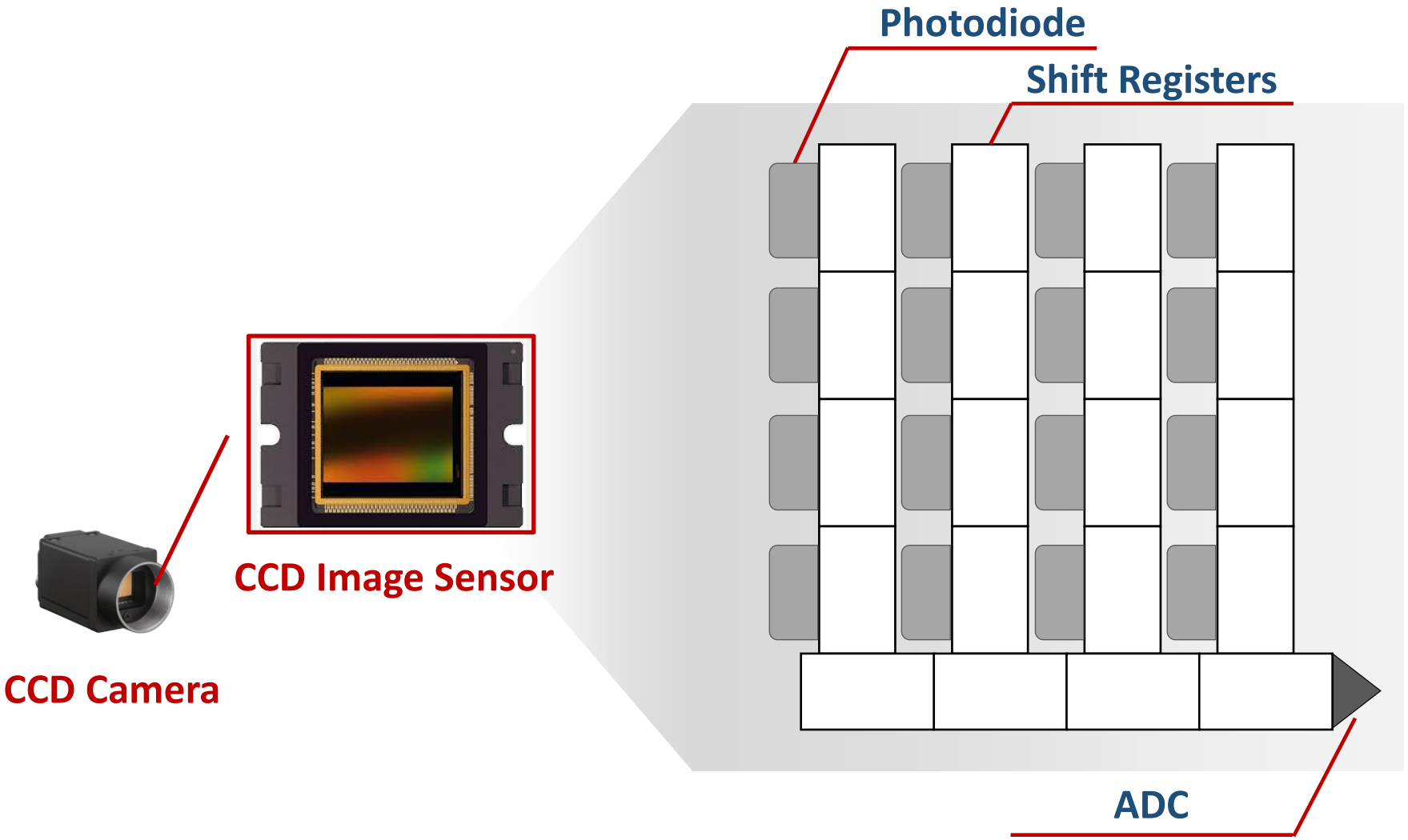
Adversary

IEMI

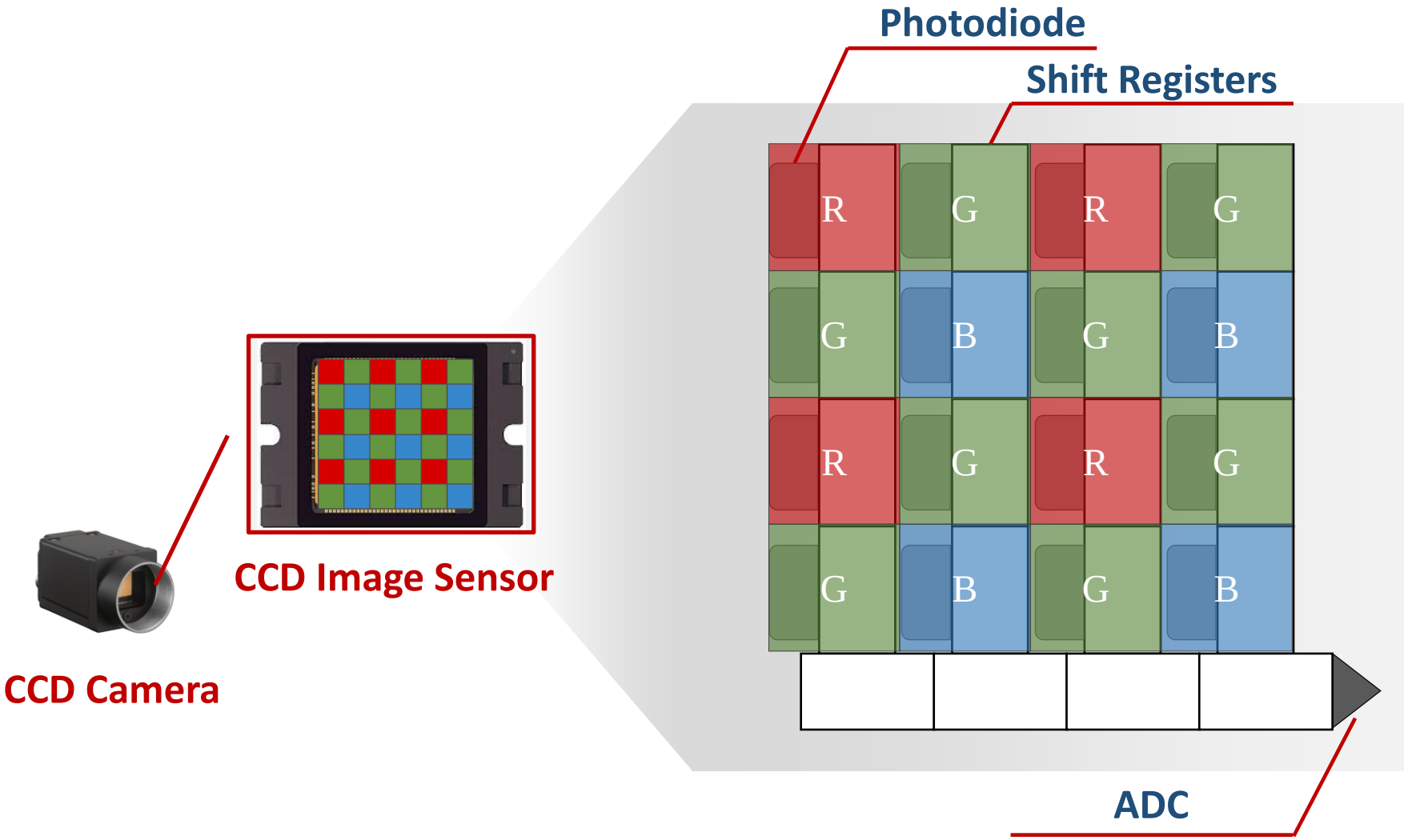
CCD Camera

Night Vision Detection	QR code scanning	Fire detection

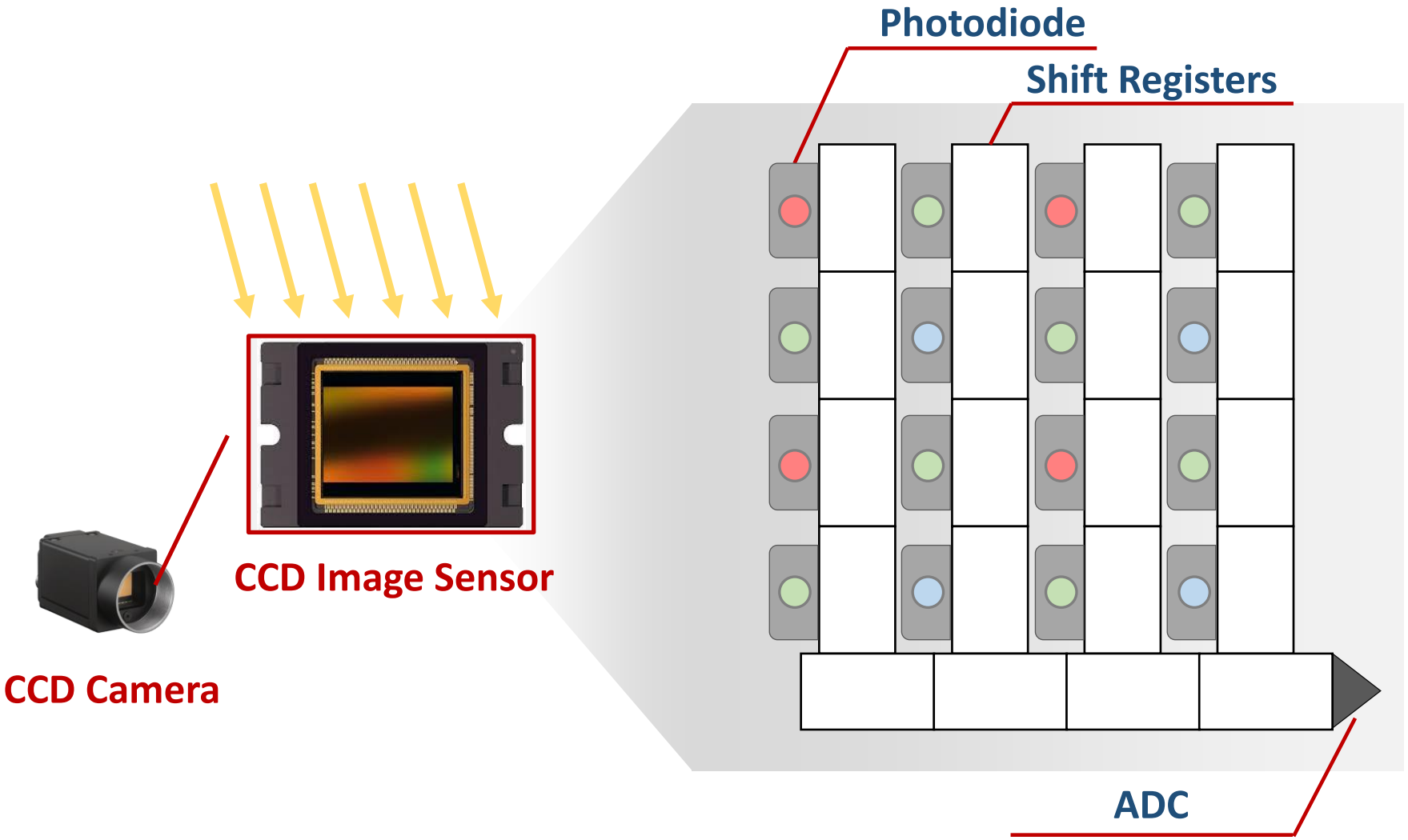
CCD Camera Mechanism



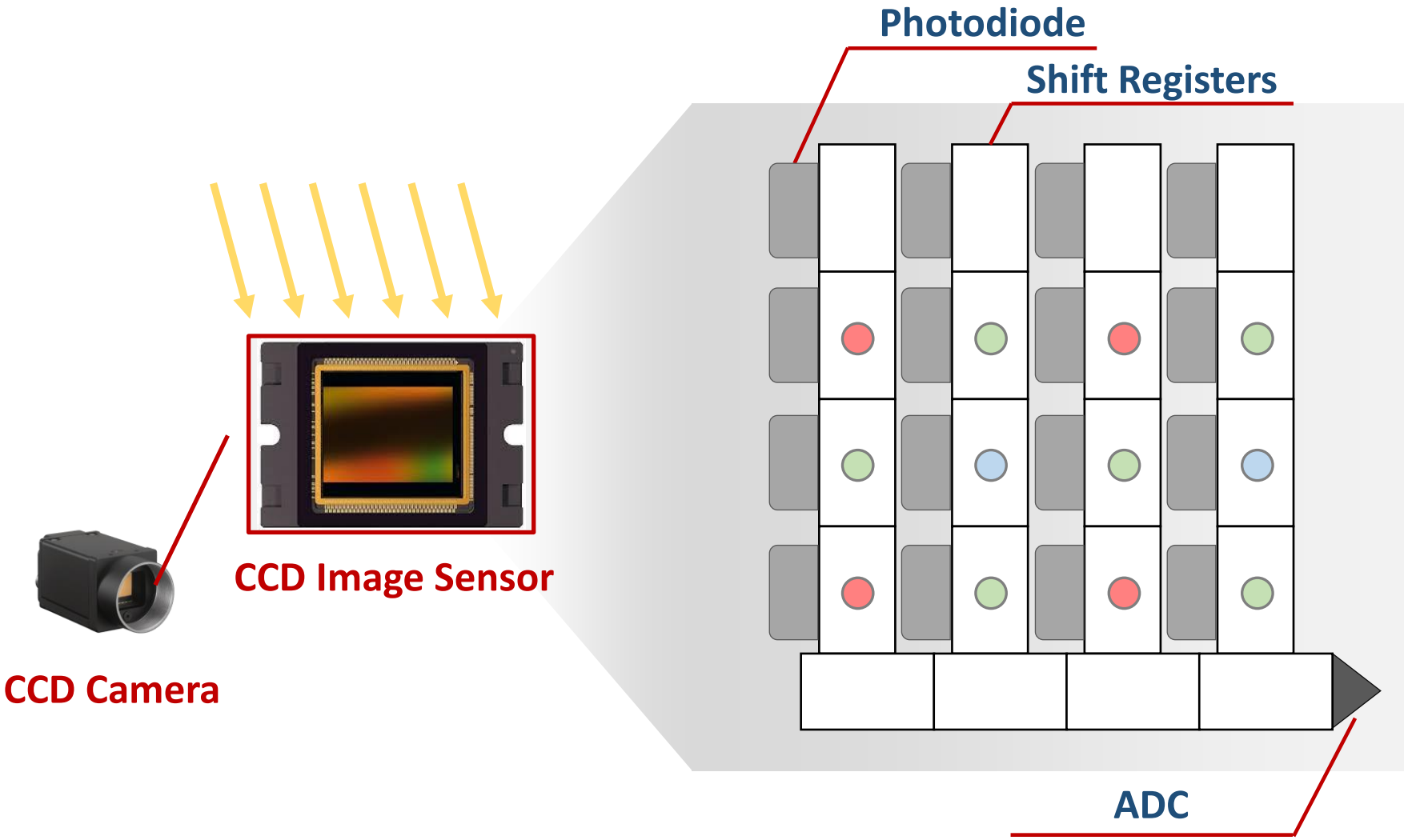
CCD Camera Mechanism



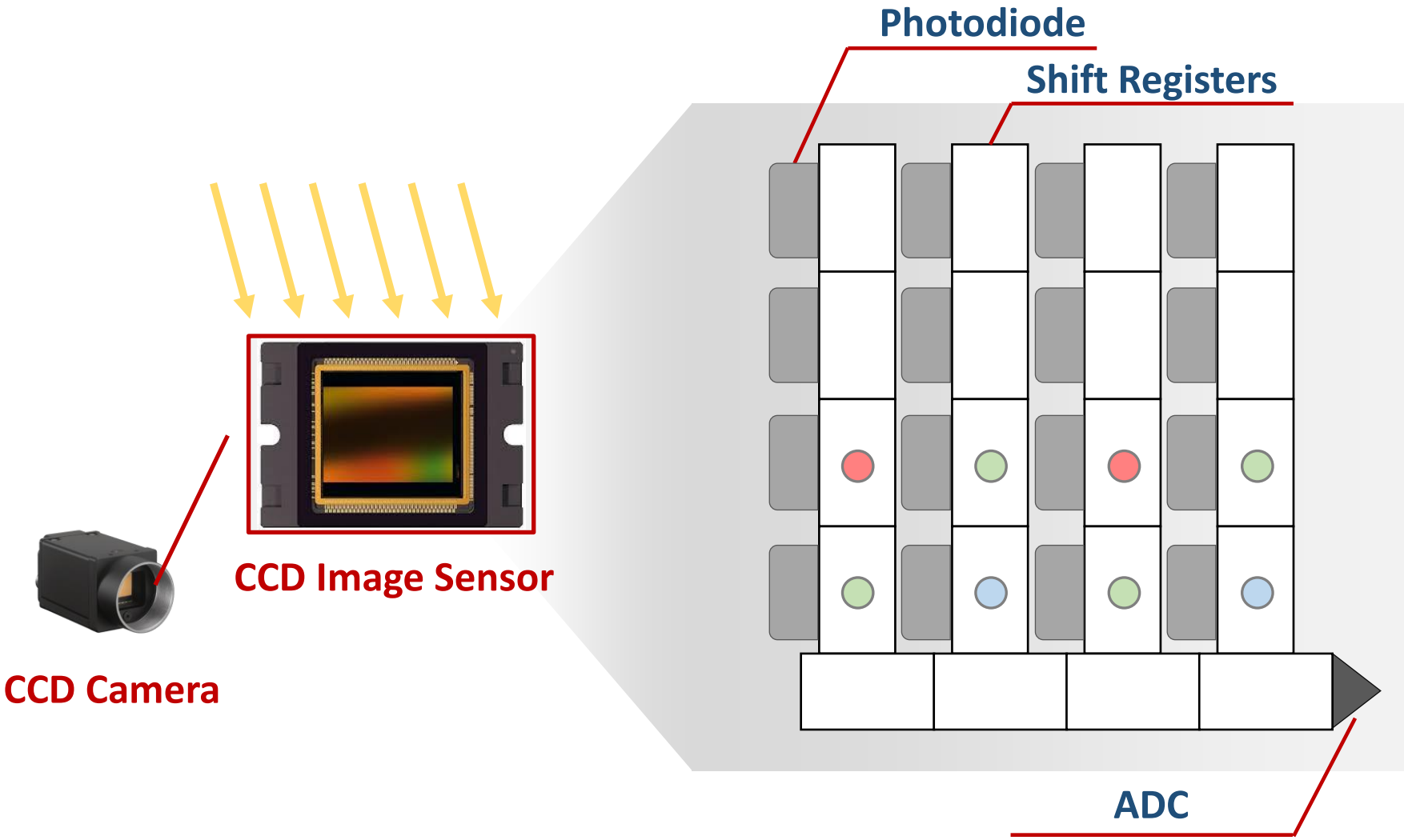
CCD Camera Mechanism



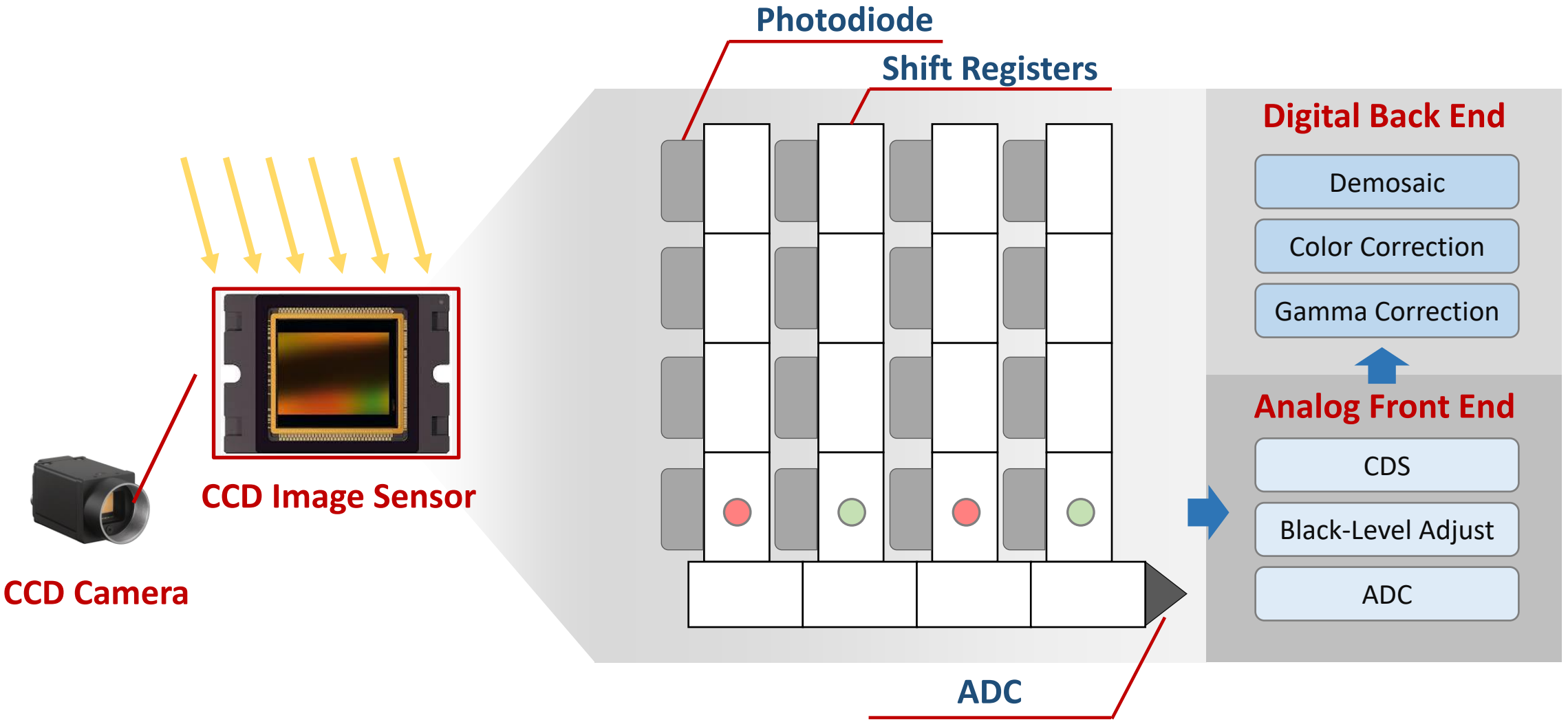
CCD Camera Mechanism



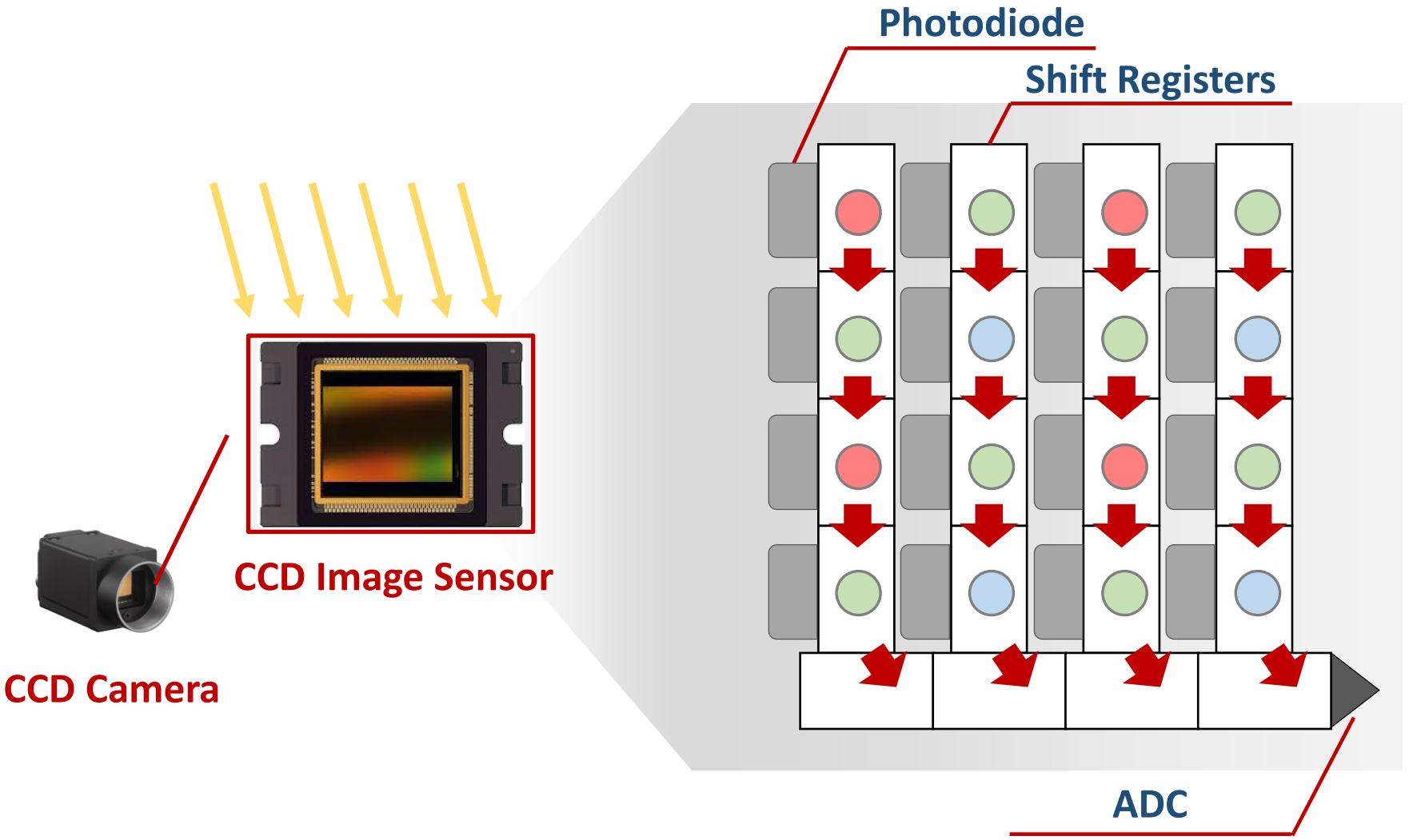
CCD Camera Mechanism



CCD Camera Mechanism

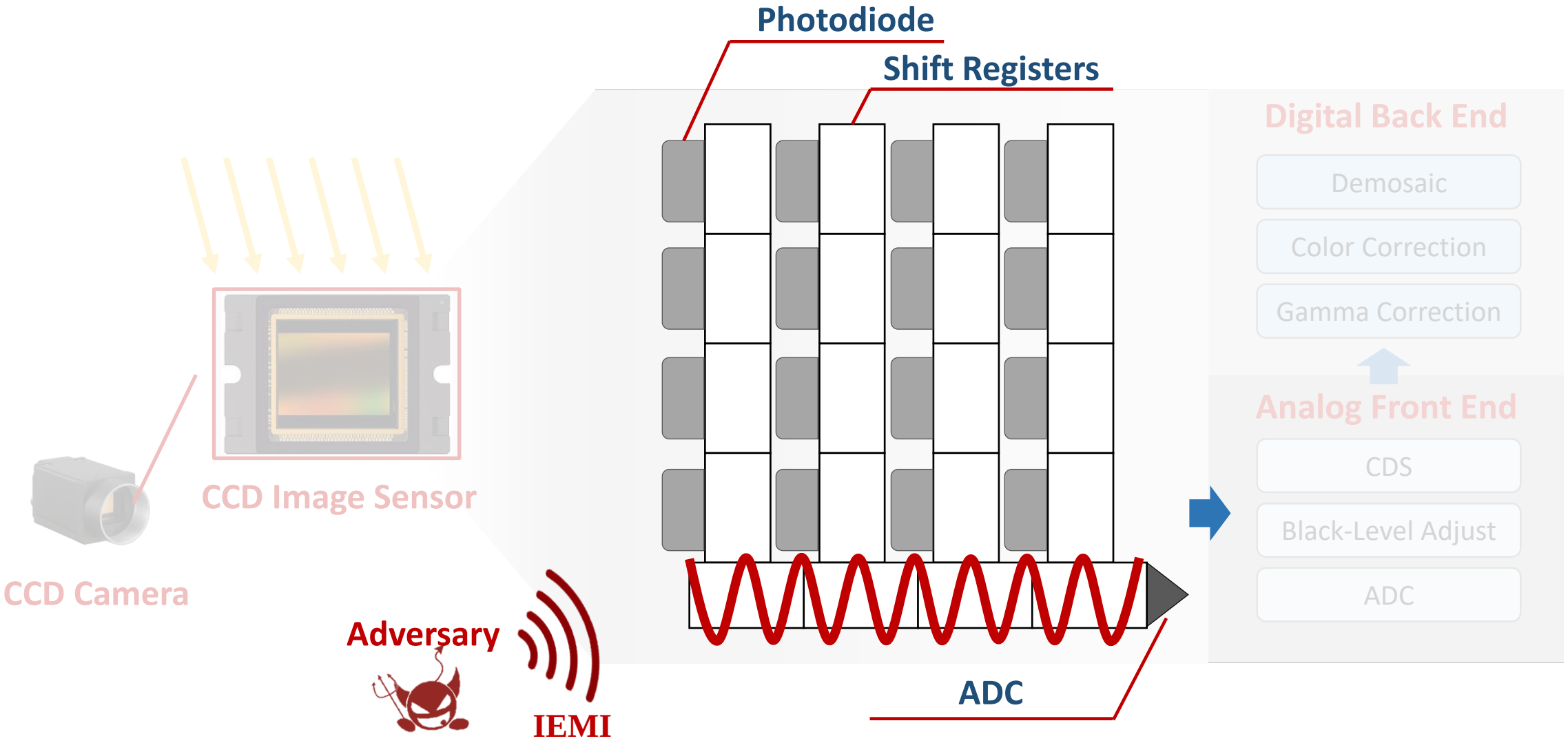


CCD Camera Mechanism

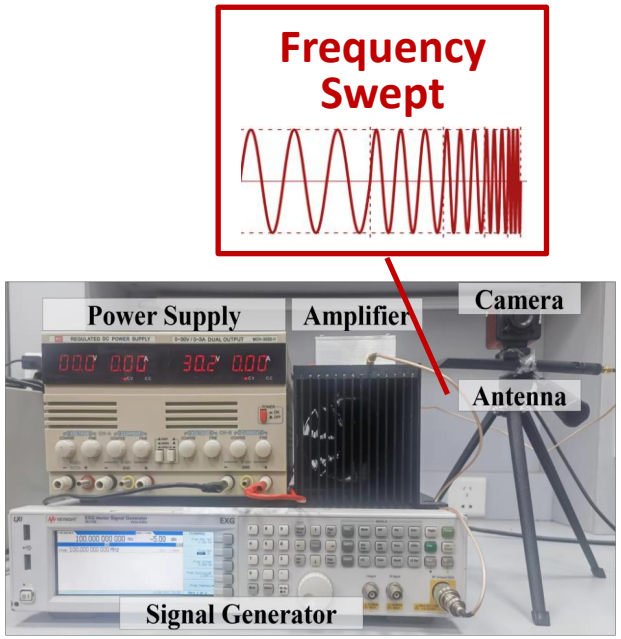


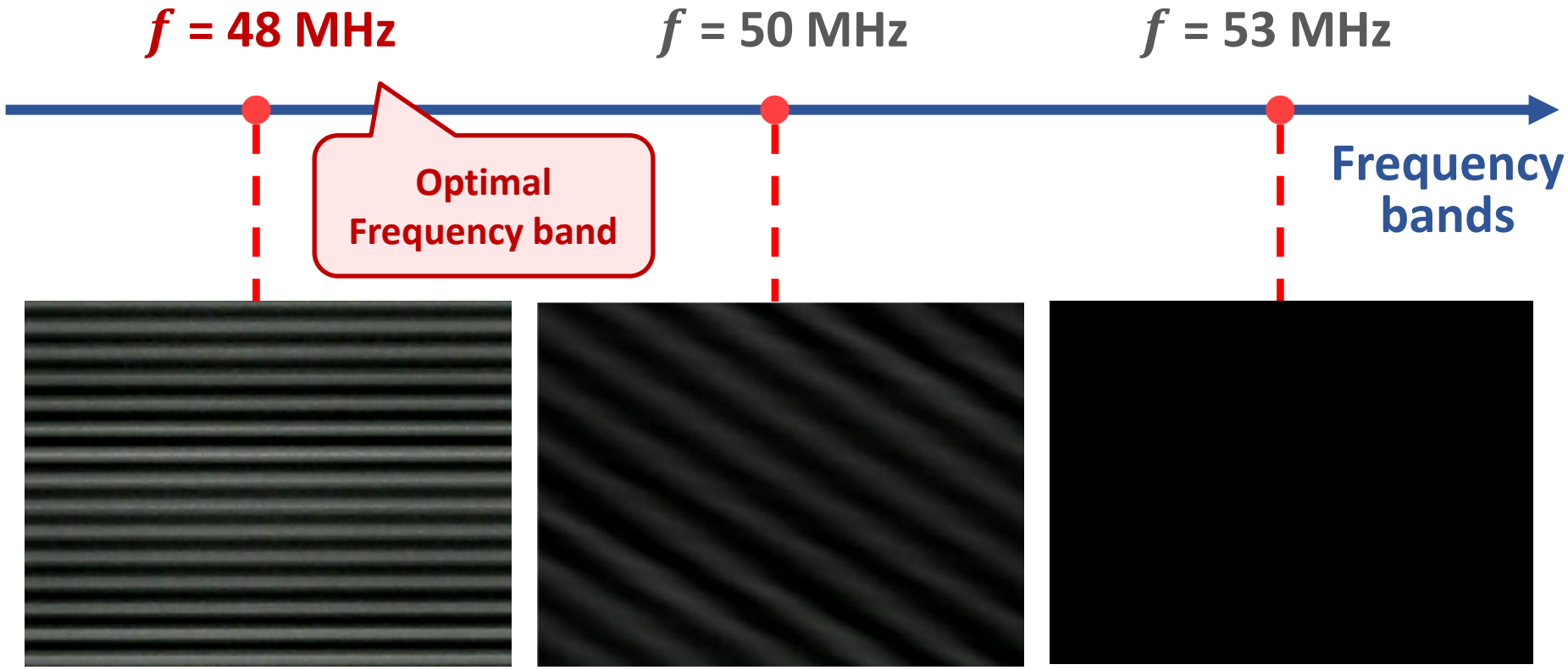
Signal Charge Readout in Order!

CCD Camera Mechanism



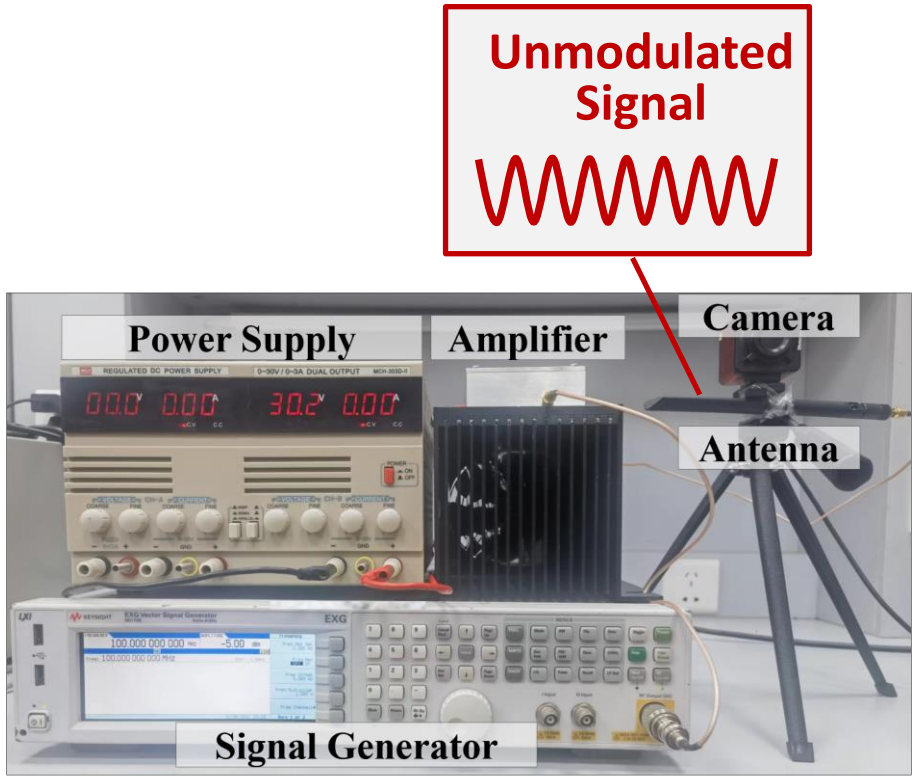
Preliminary Experiments

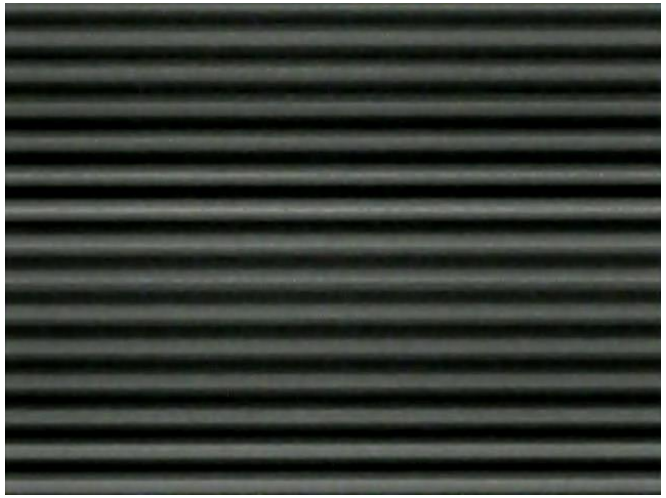




The **optimal frequency band** depends on the **coupling frequency** of the **camera's internal circuitry**

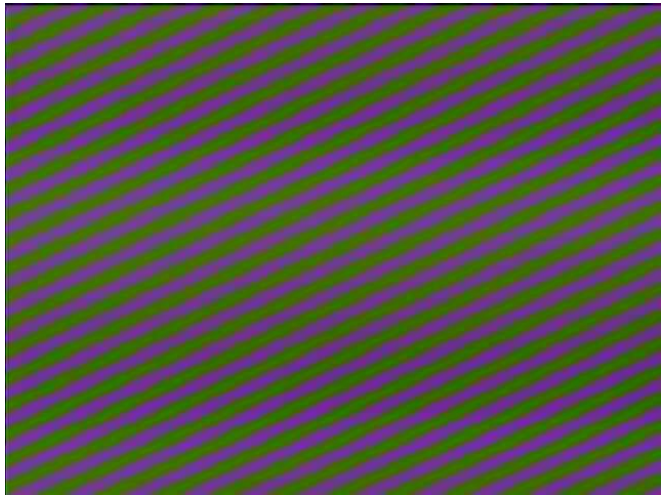
Preliminary Experiments



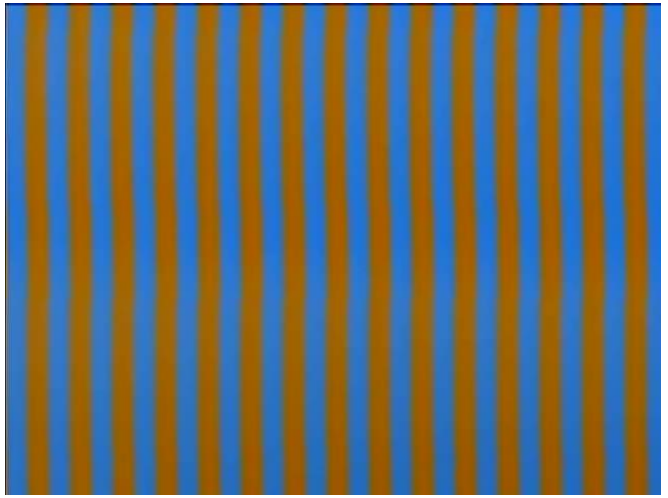


f = 48.0000 MHz

f = 48.0038 MHz

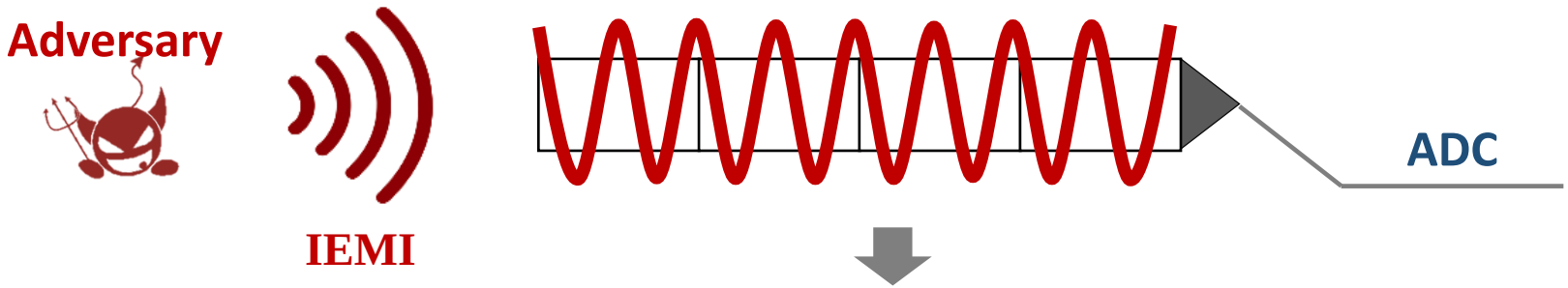


f = 54.0325 MHz

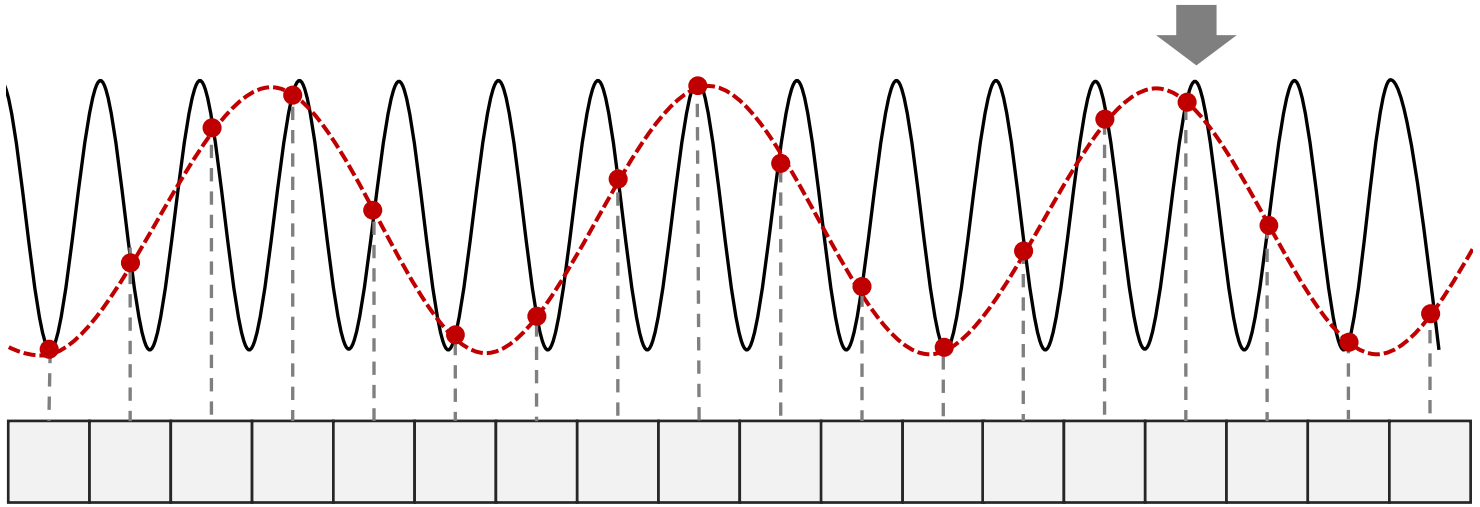


f = 54.0688 MHz

Sampling and Aliasing



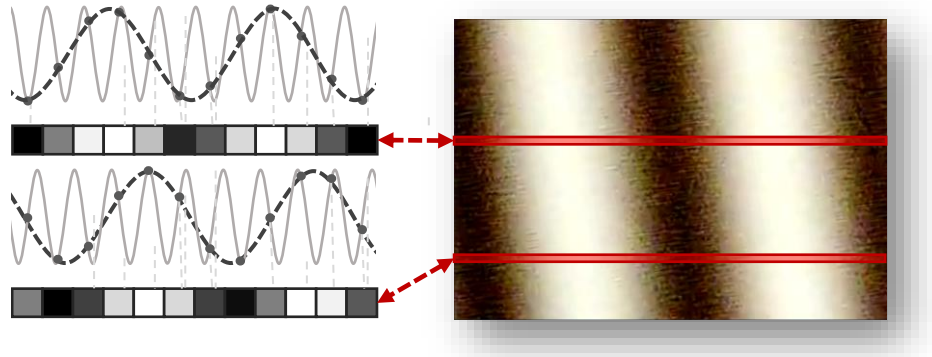
Aliasing Effect



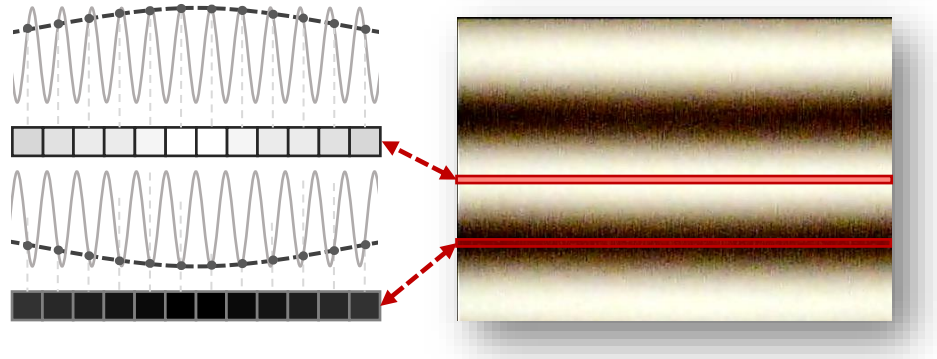
$$f_{alias} = |f_{in} - N \times f_s|$$

Causality of Stripes

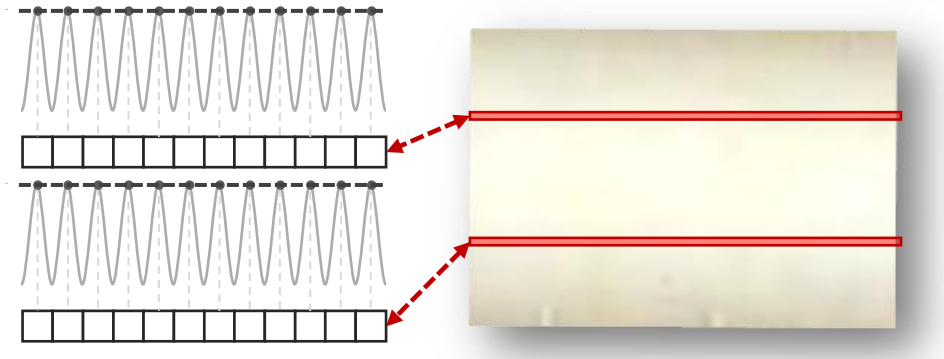
When $f_{alias} \geq f_{row}$ → $f_{alias} = 2.16\, f_{row}$



When $f_{alias} < f_{row}$ → $f_{alias} = 0.006\, f_{row}$



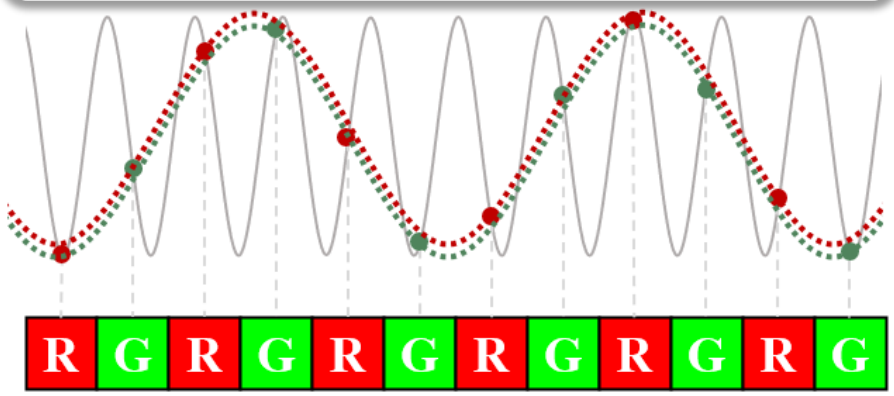
When $f_{alias} = 0$ → $f_{alias} = 0$

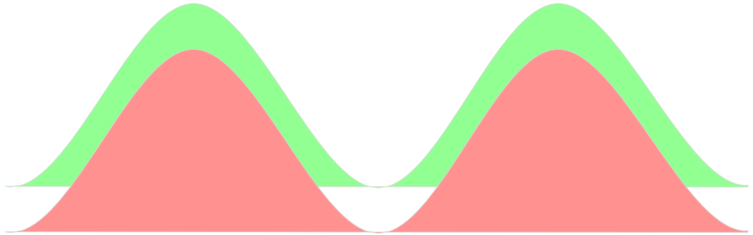


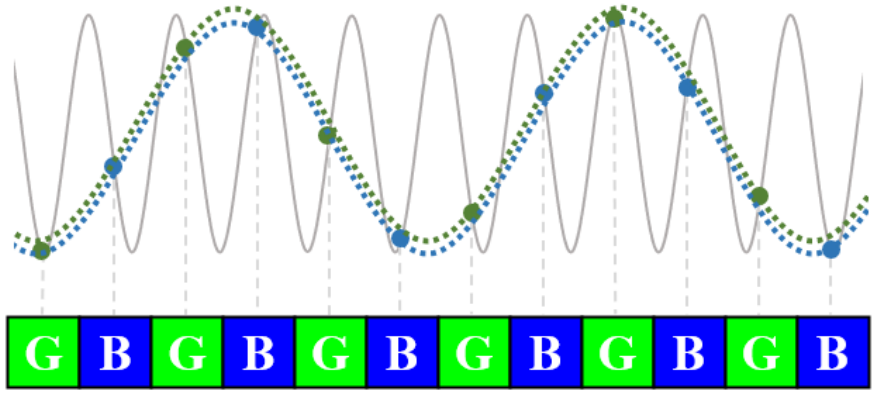
Causality of Color Stripes

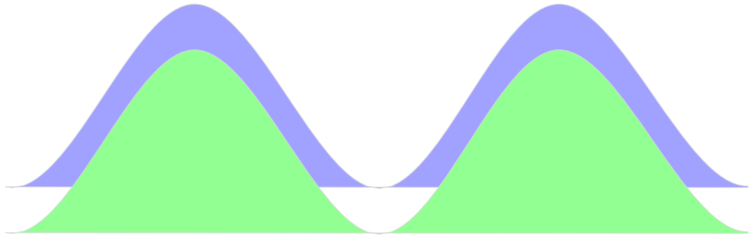
When $f_{in} = N \times f_s \mp \Delta f$

$$f_{alias} = |f_{in} - N \times f_s| = \Delta f$$





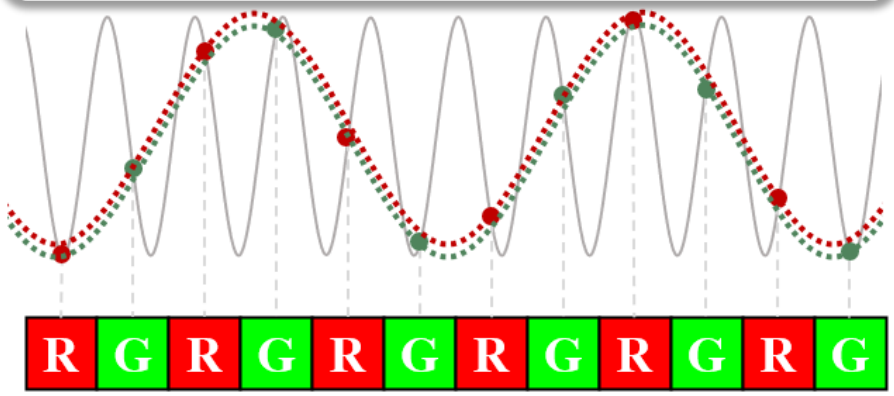


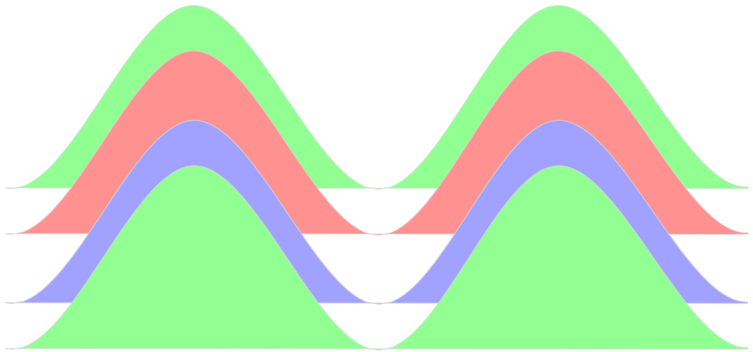


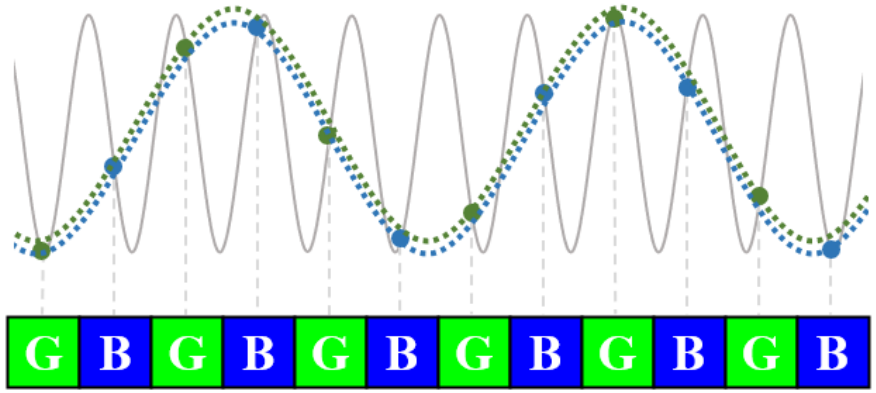
Causality of Color Stripes

When $f_{in} = N \times f_s \mp \Delta f$

$$f_{alias} = |f_{in} - N \times f_s| = \Delta f$$



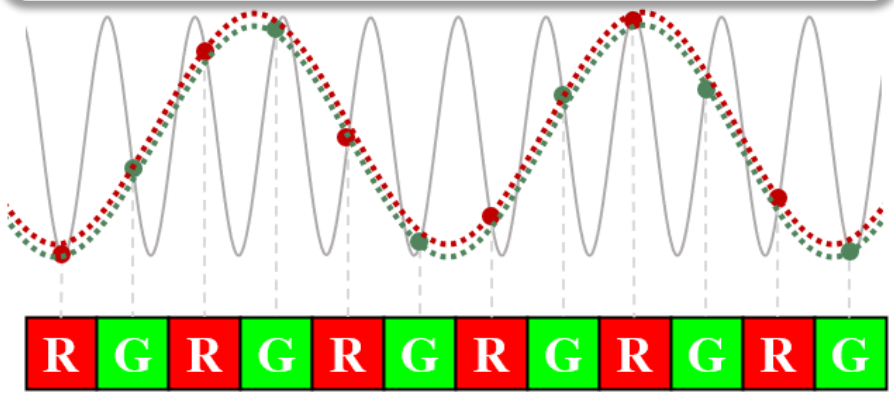


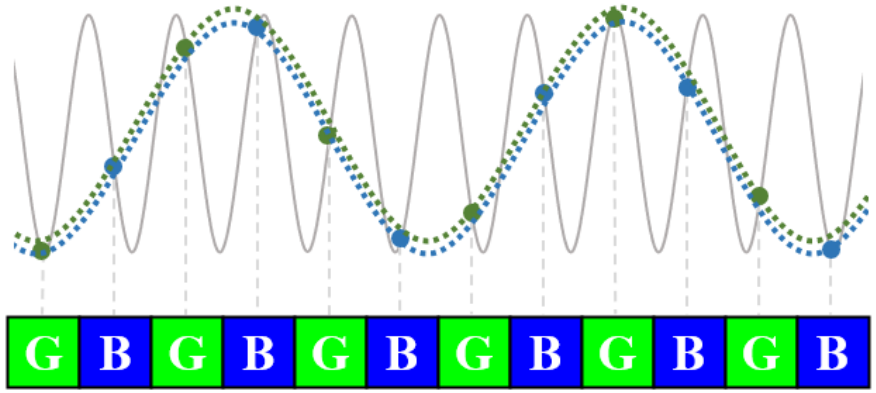


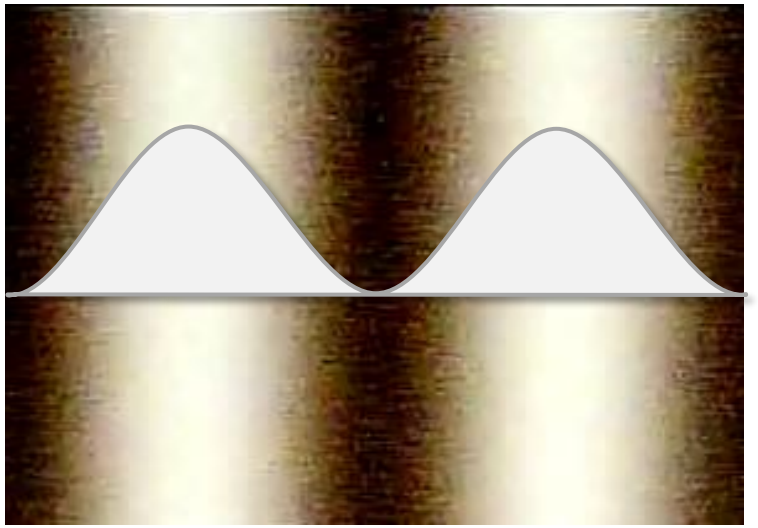
Causality of Color Stripes

When $f_{in} = N \times f_s \mp \Delta f$

$$f_{alias} = |f_{in} - N \times f_s| = \Delta f$$



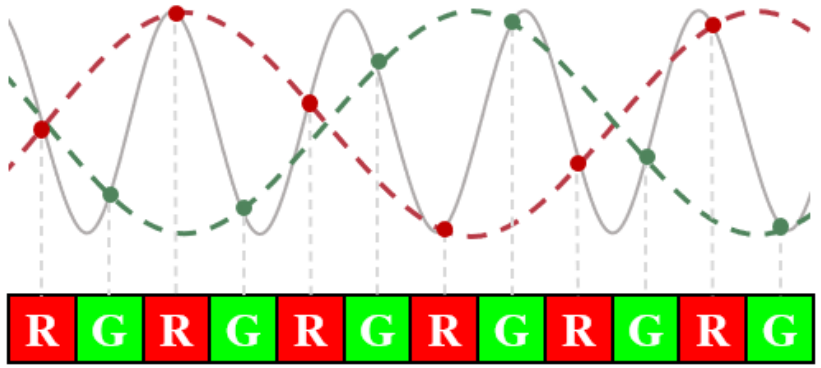


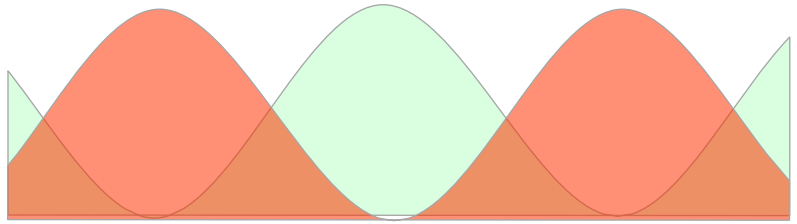


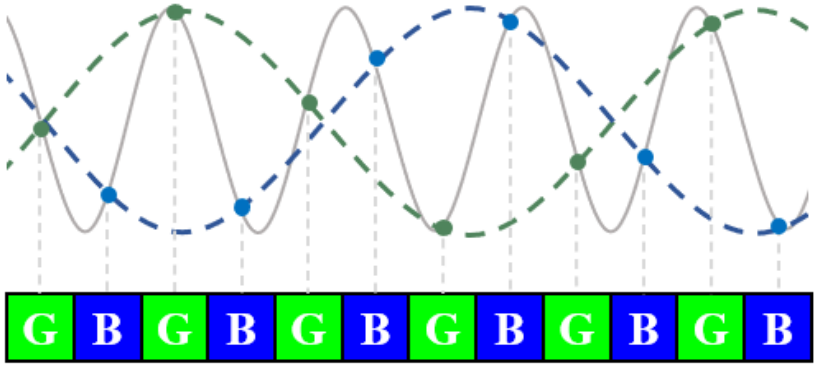
Causality of Coloration

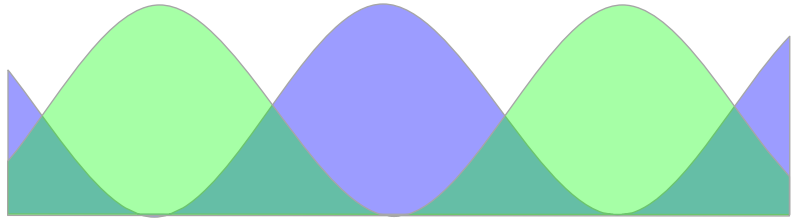
When $f_{in} = \frac{N}{2} \times f_s \mp \Delta f$

$$f_{alias} = |f_{in} - N \times f_s| = \frac{f_s}{2} \mp \Delta f$$





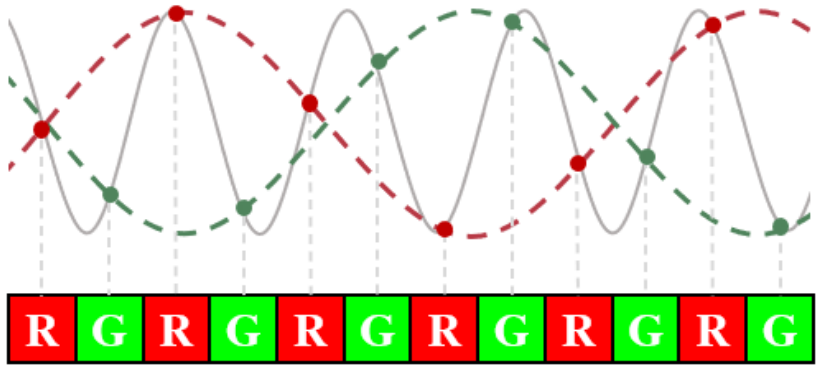


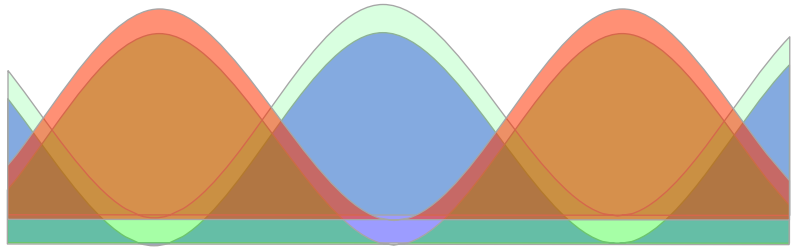


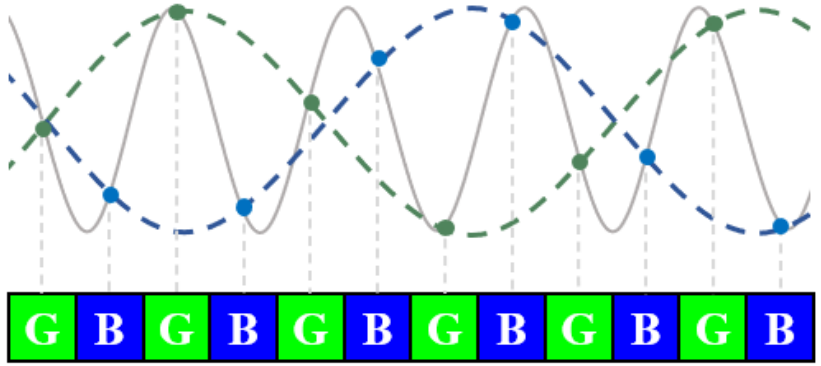
Causality of Coloration

When $f_{in} = \frac{N}{2} \times f_s \mp \Delta f$

$$f_{alias} = |f_{in} - N \times f_s| = \frac{f_s}{2} \mp \Delta f$$



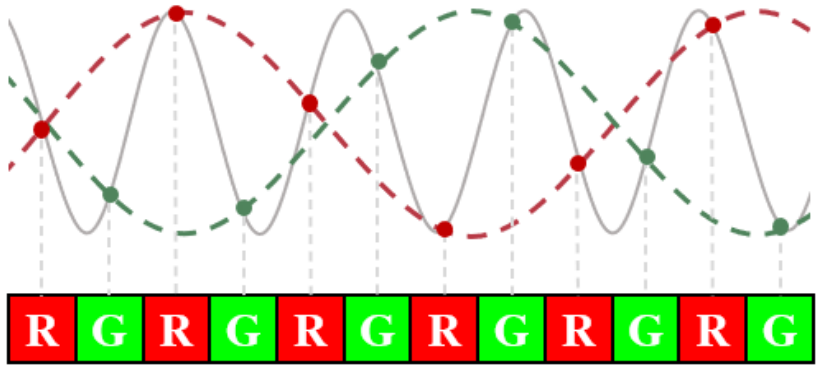


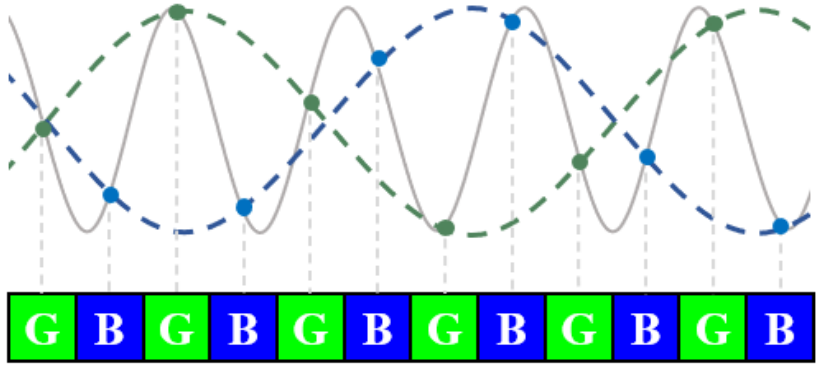


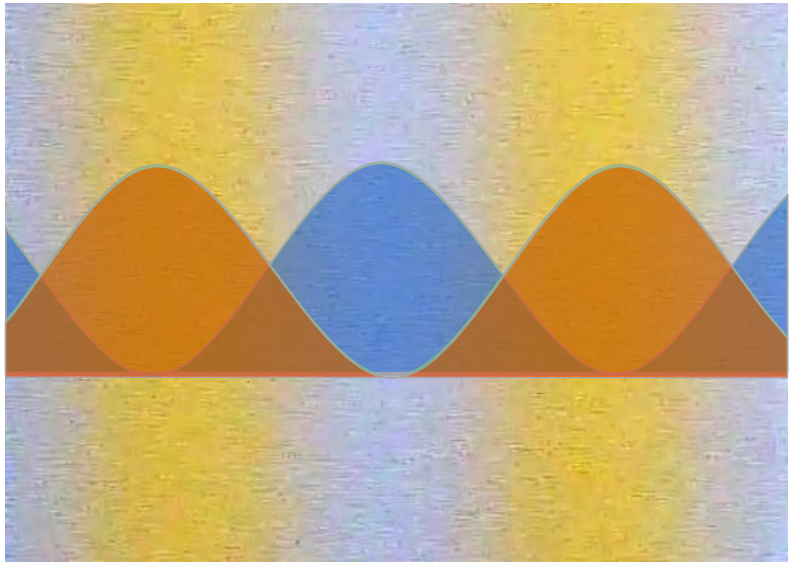
Causality of Coloration

When $f_{in} = \frac{N}{2} \times f_s \mp \Delta f$

$$f_{alias} = |f_{in} - N \times f_s| = \frac{f_s}{2} \mp \Delta f$$

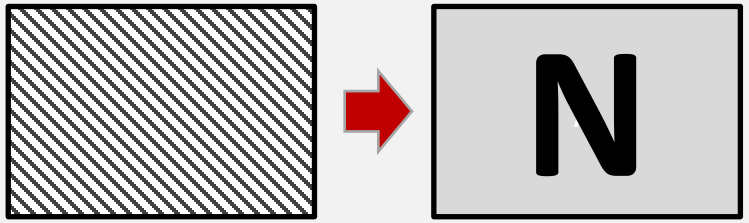




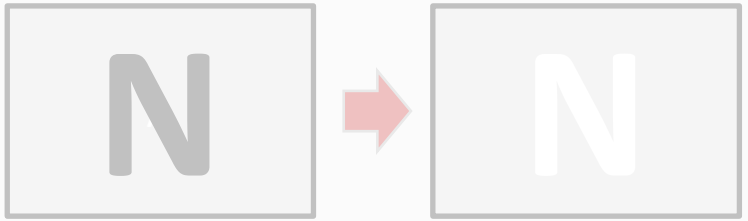


Ability Investigation

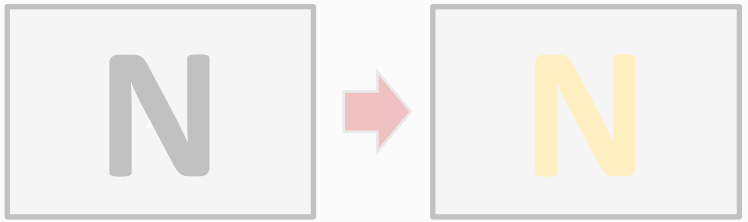
Q1: How to control the **morphology** of the injection?



Q2: How to control the **brightness** of the injection?

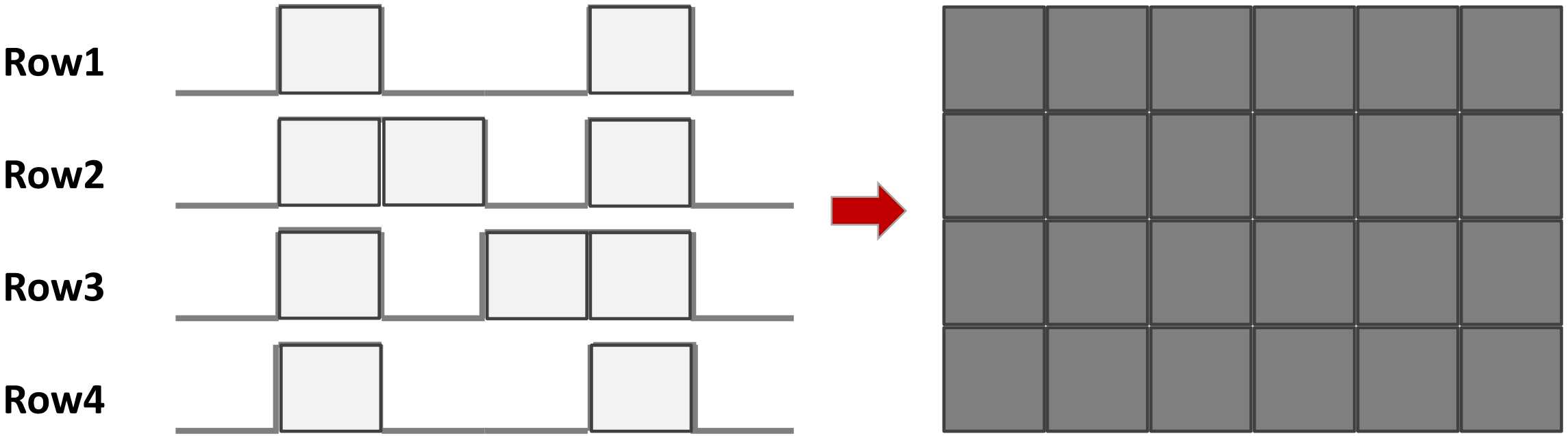


Q3: How to control the **color** of the injection?



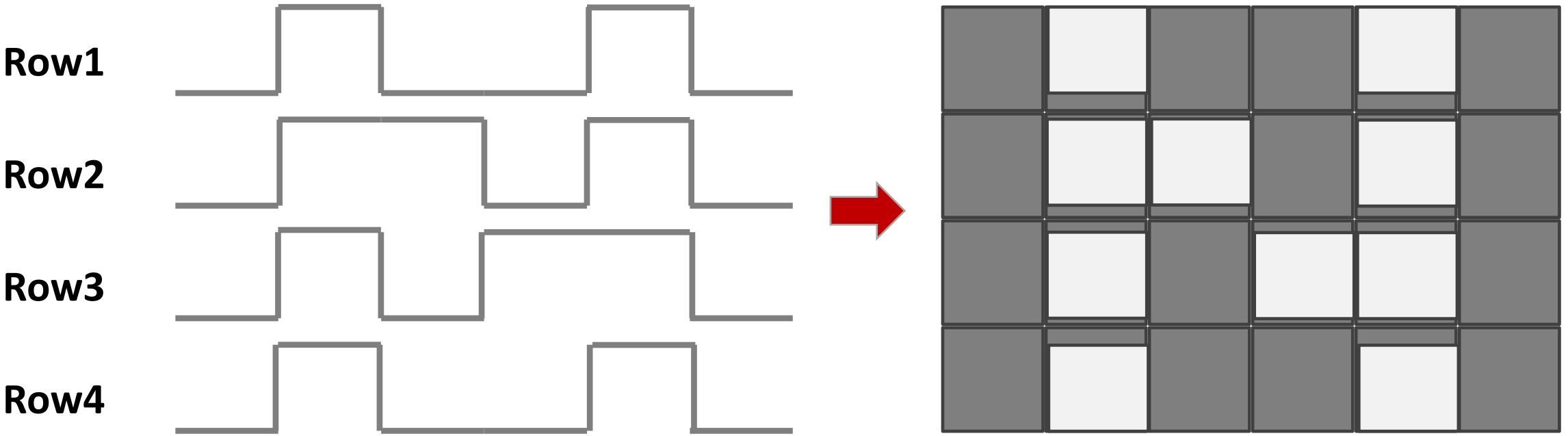
Morphology Modulations

Amplitude Modulation



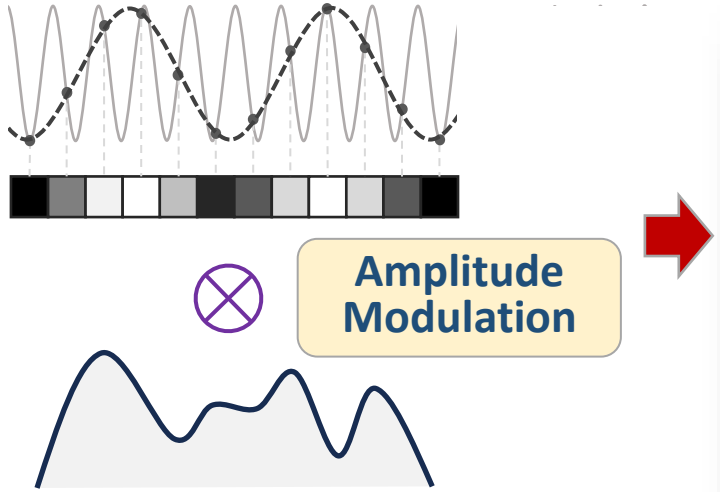
Morphology Modulations

Amplitude Modulation

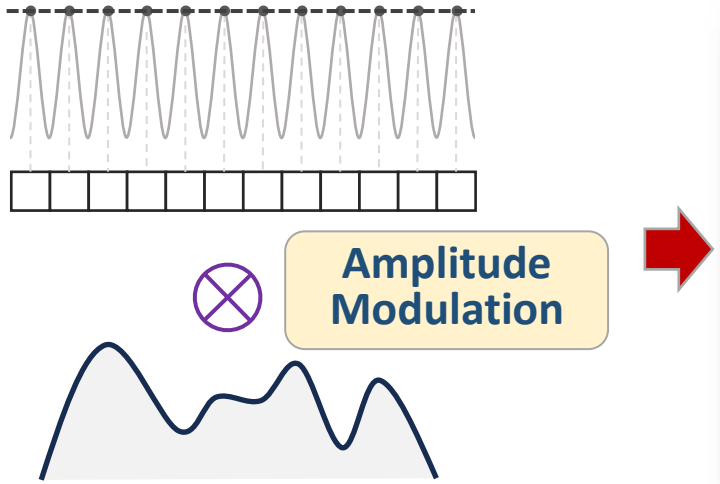


Morphology Modulations

When $f_{alias} \geq f_{row}$

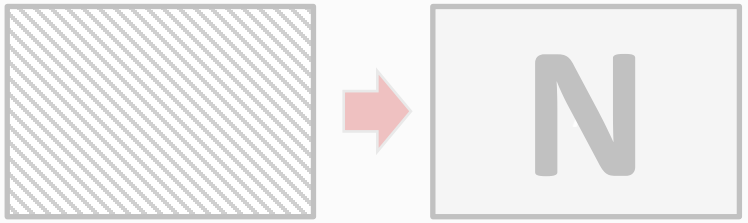


When $f_{in} = N \times f_s$

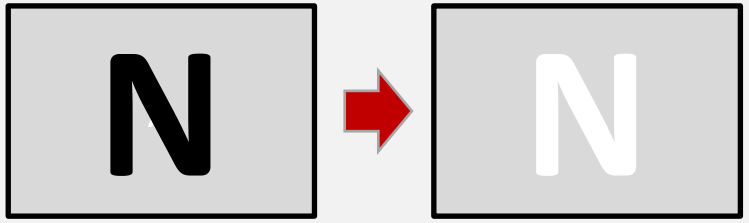


Ability Investigation

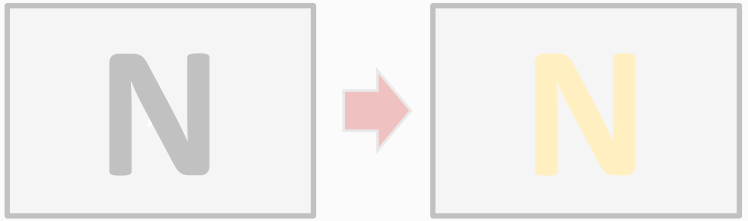
Q1: How to control the **morphology** of the injection?



Q2: How to control the **brightness** of the injection?

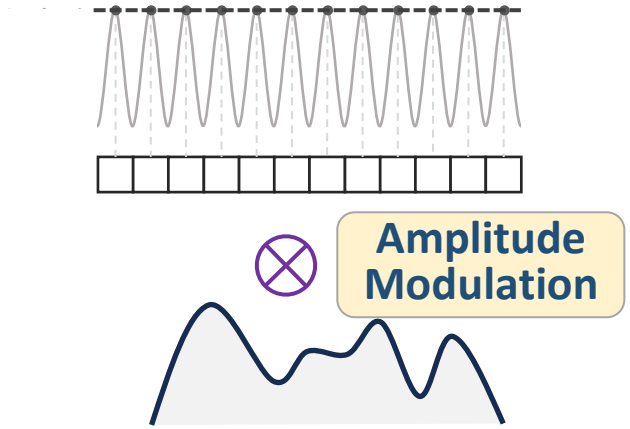


Q3: How to control the **color** of the injection?

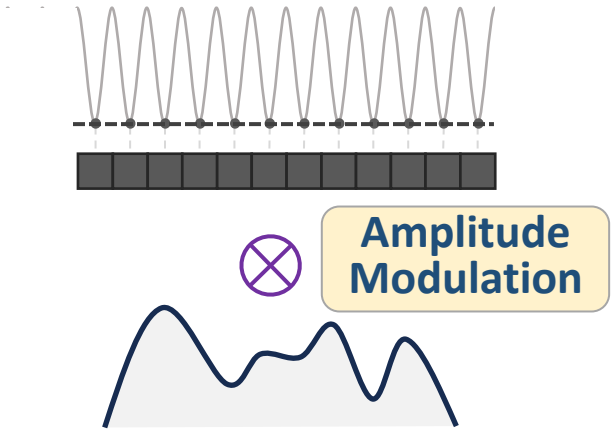


Brightness Modulations

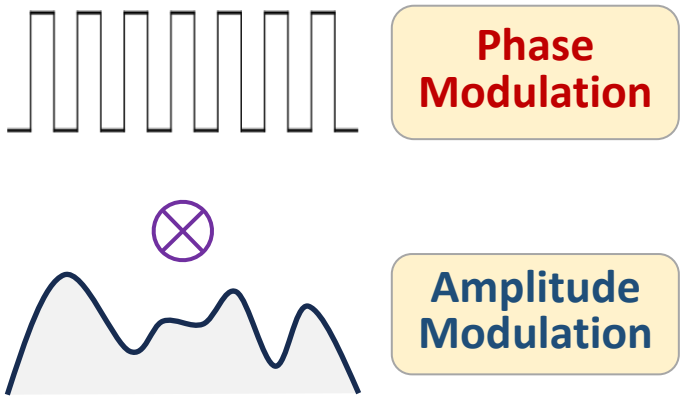
When $\varphi_0 > 0$



When $\varphi_0 < 0$

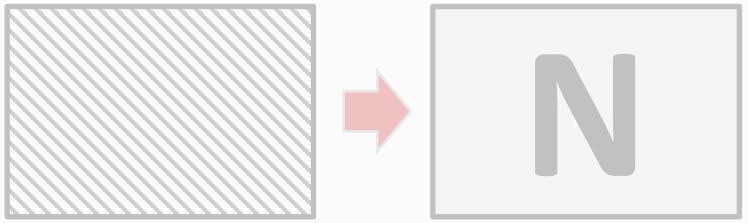


Phase Modulation

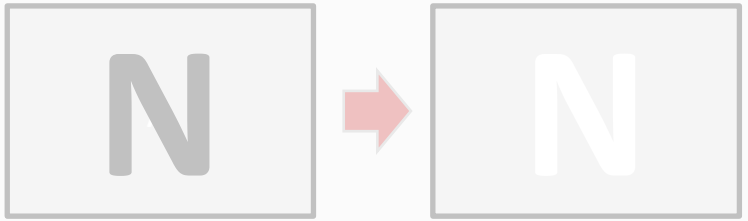


Ability Investigation

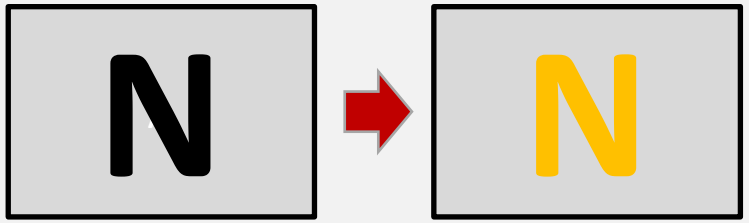
Q1: How to control the **morphology** of the injection?



Q2: How to control the **brightness** of the injection?

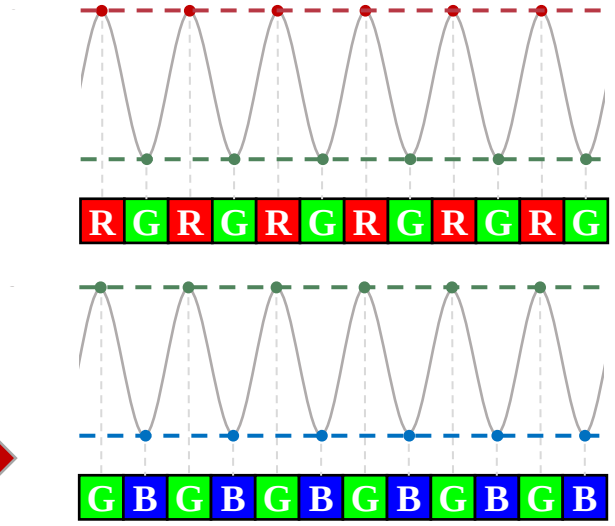


Q3: How to control the **color** of the injection?



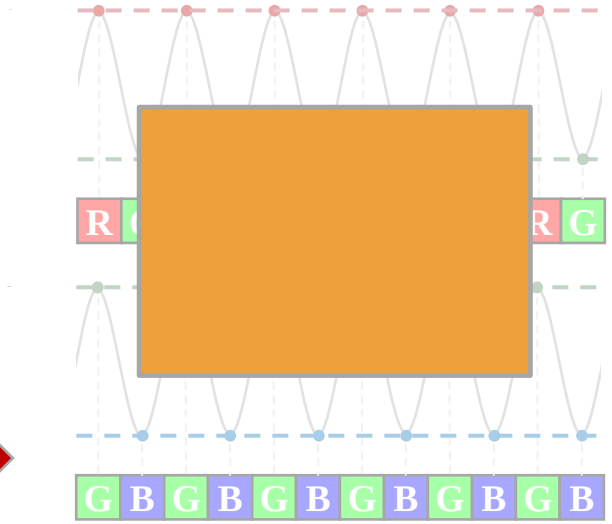
Coloration Modulations

When $f_{in} = N \times \frac{f_s}{2}$



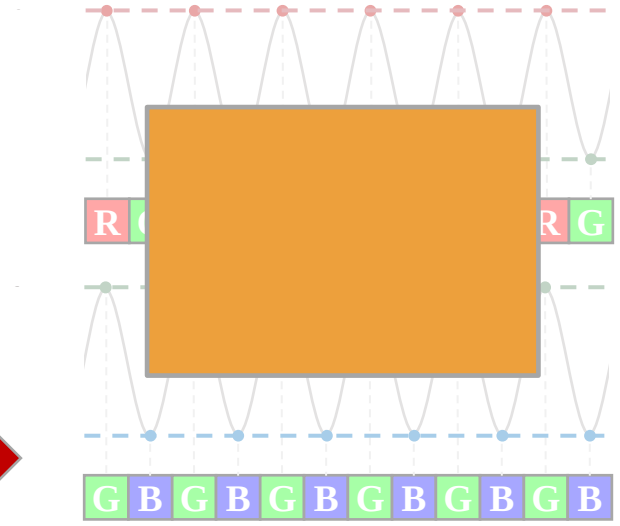
Coloration Modulations

When $f_{in} = N \times \frac{f_s}{2}$

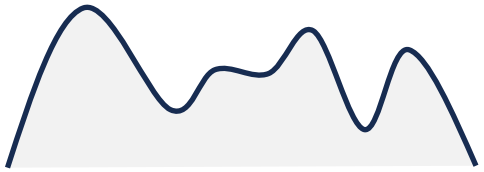


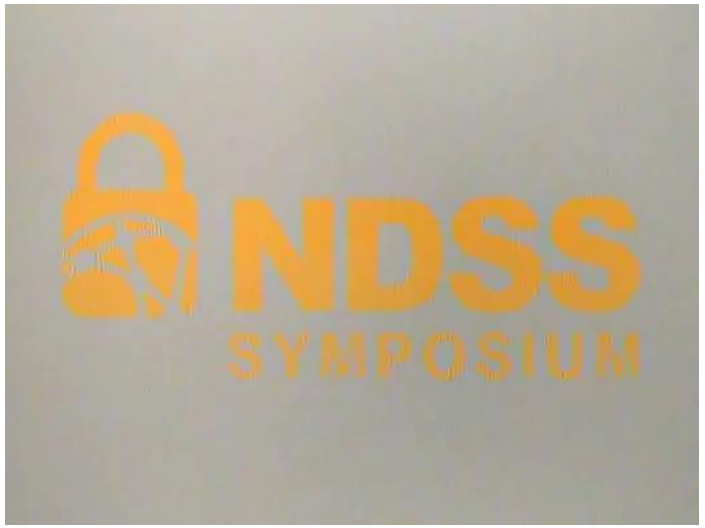
Coloration Modulations

When $f_{in} = N \times \frac{f_s}{2}$



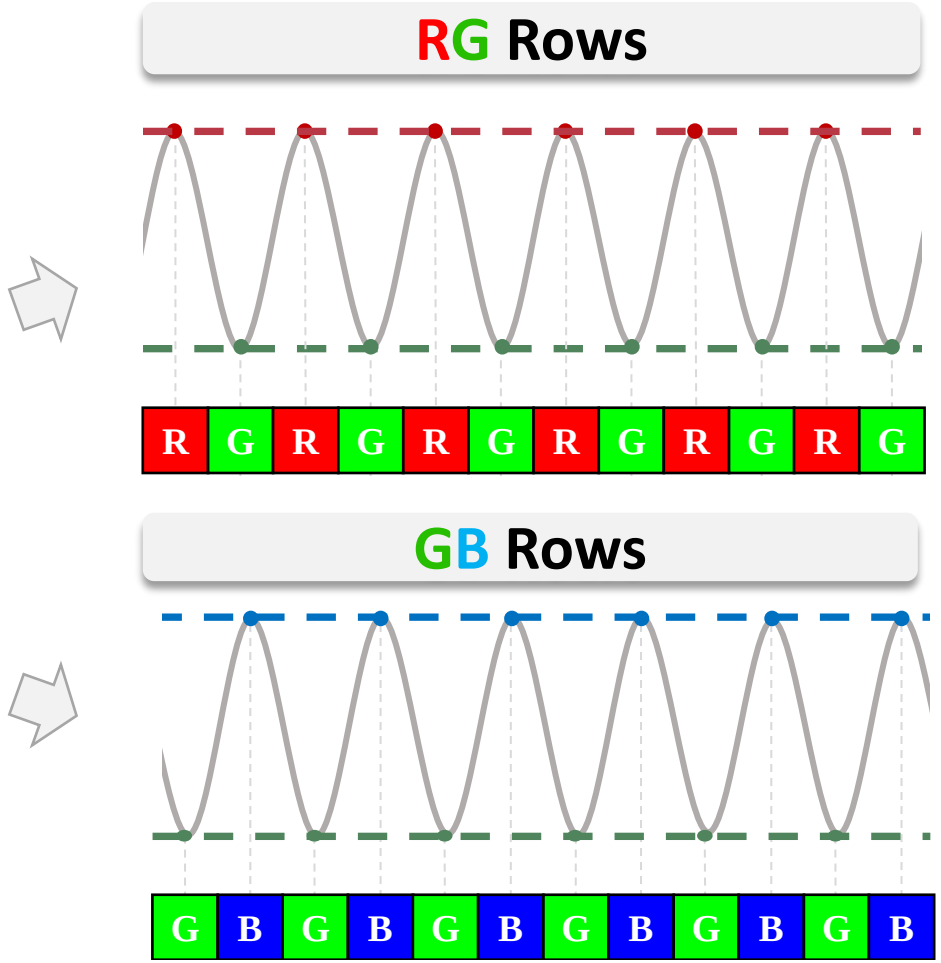
Amplitude Modulation

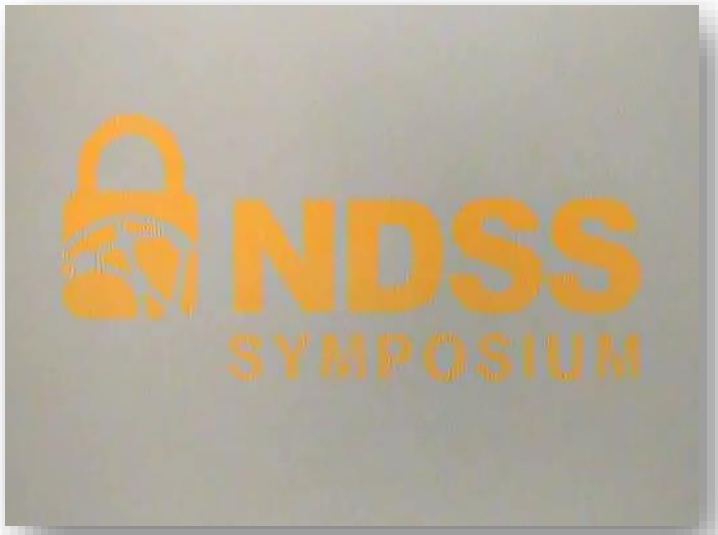




Coloration Modulations

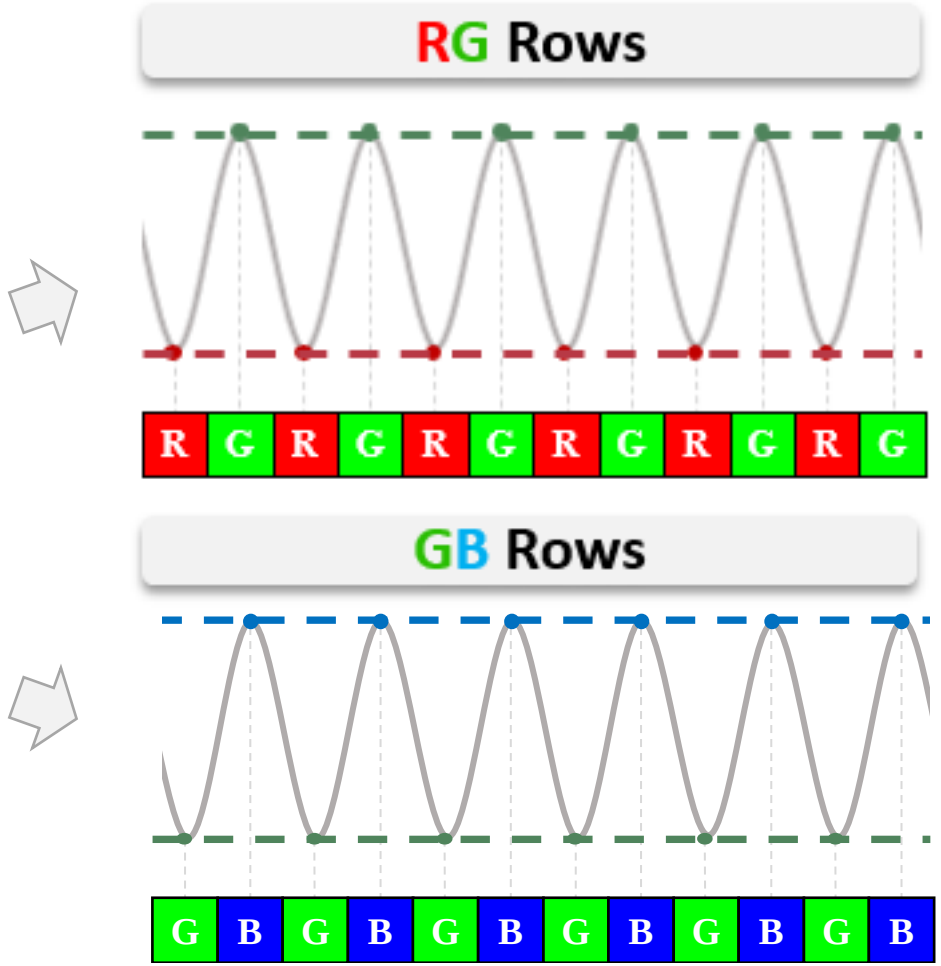
When $f_{in} = N \times \frac{f_s}{2}$



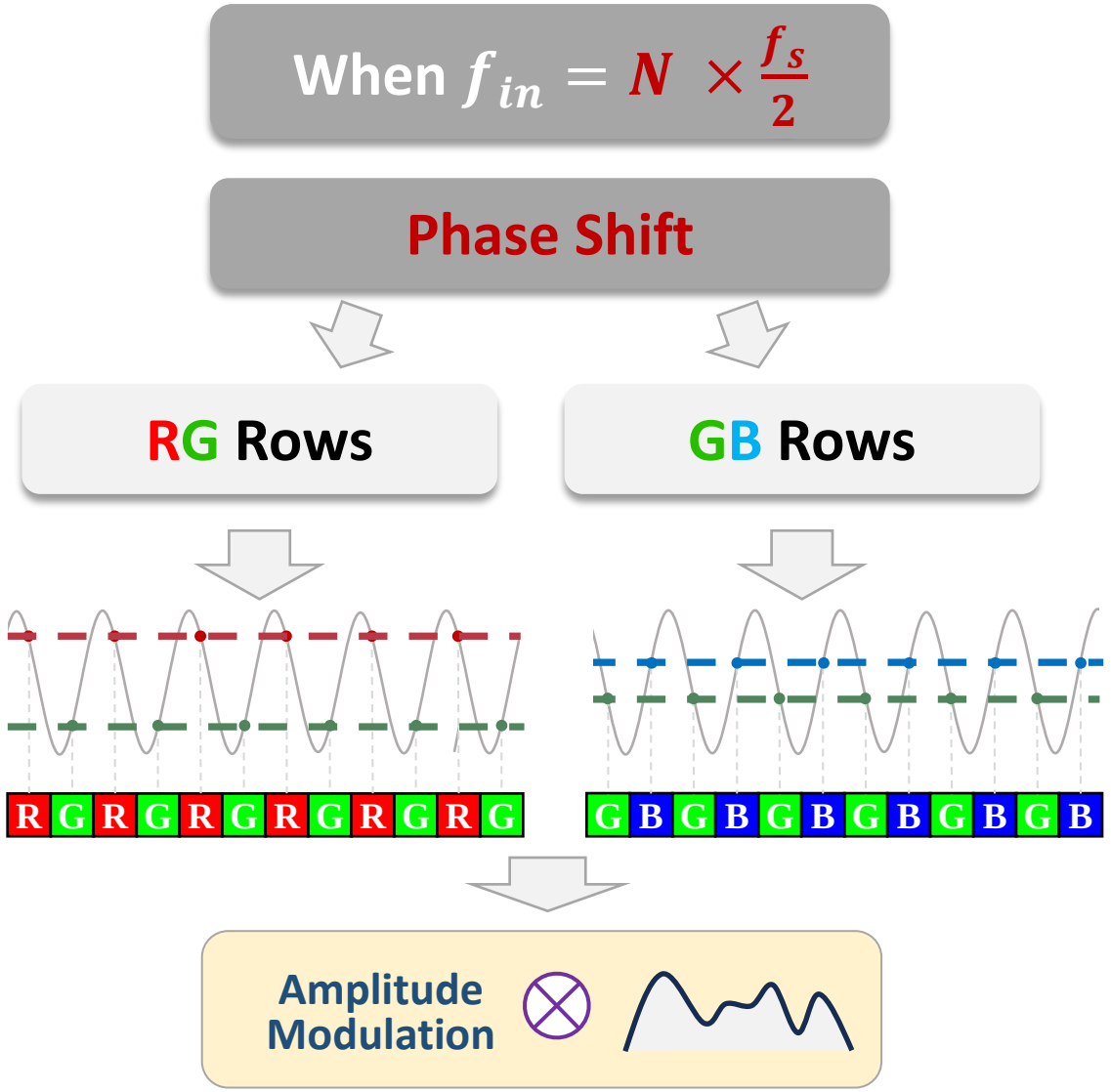


Coloration Modulations

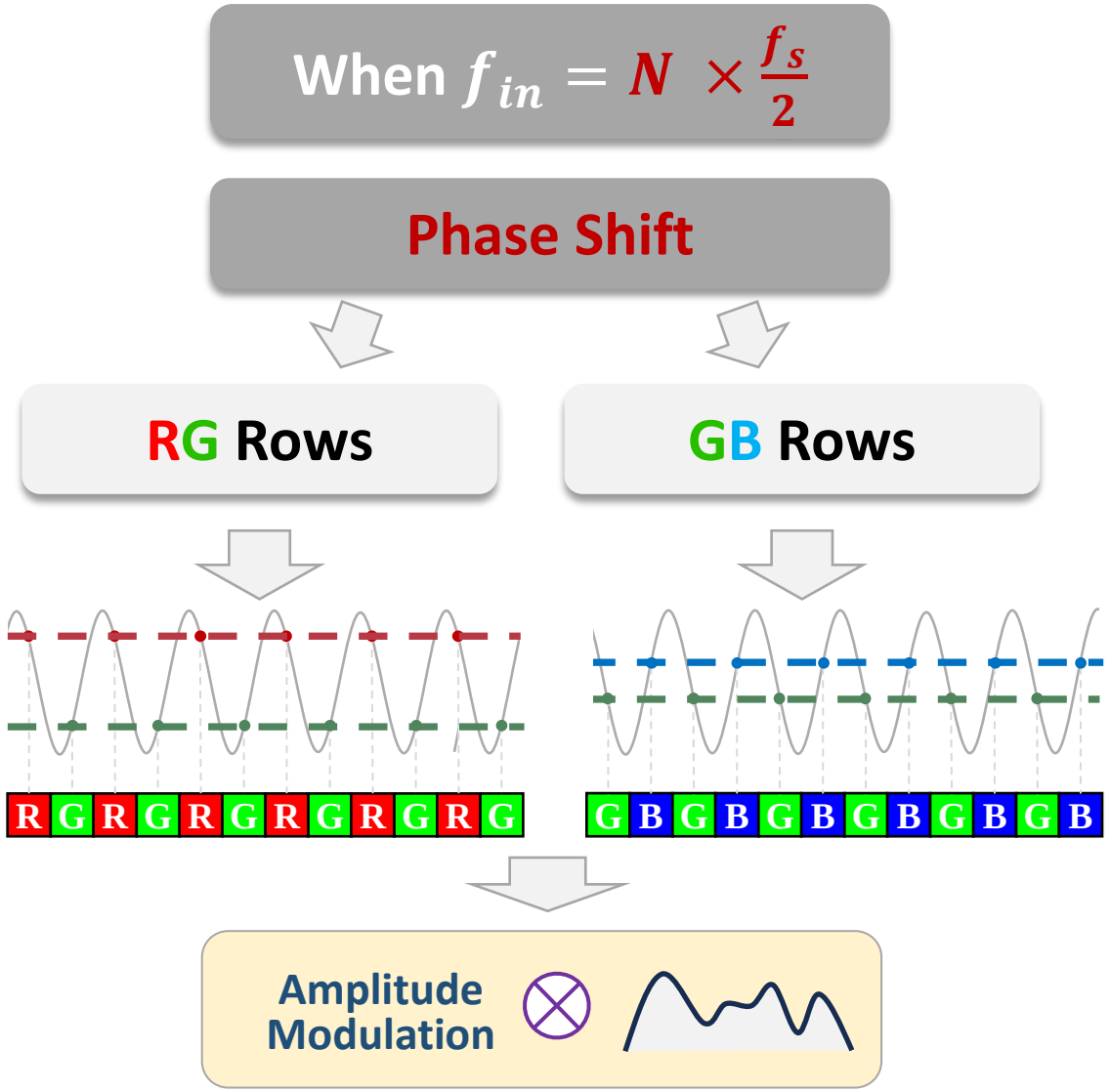
When $f_{in} = N \times \frac{f_s}{2}$



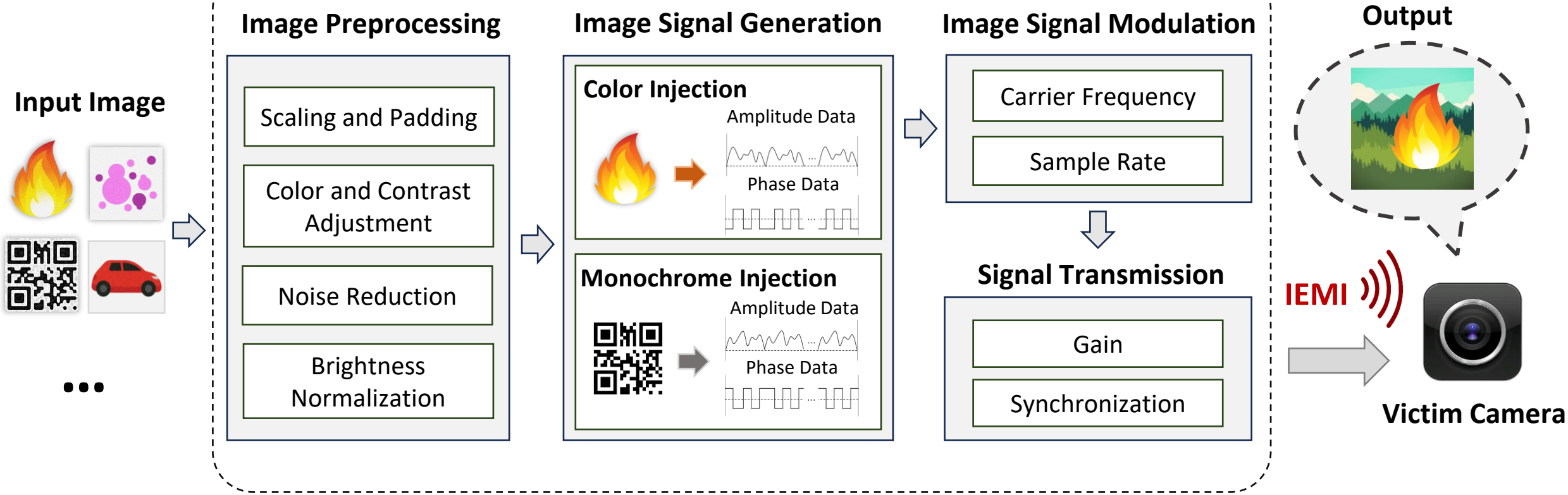
Coloration Modulations



Coloration Modulations



Attack Design



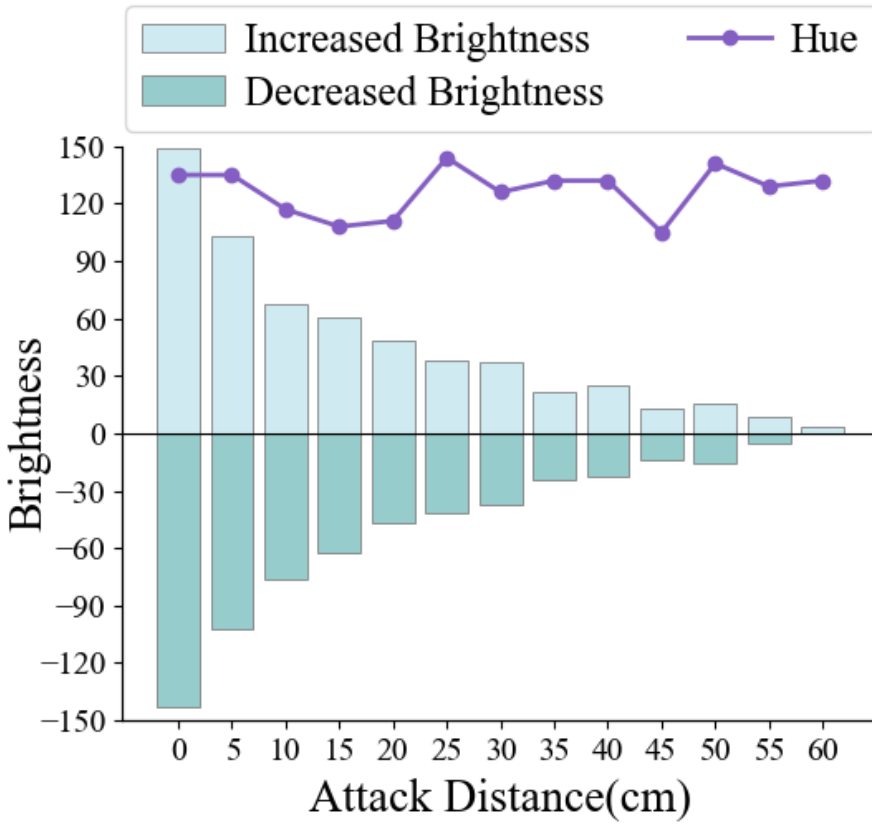
Attack on Various Cameras

We successfully perform **color** or **monochrome** injection attacks on **15 CCD cameras.**

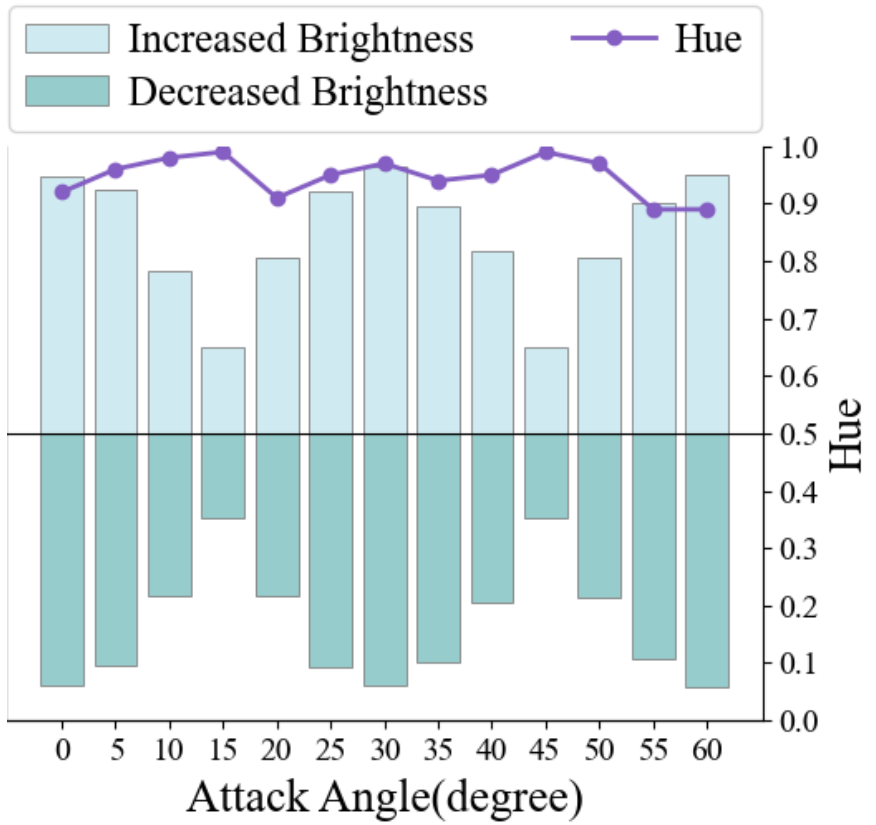
CCD Camera System and Sensor Configureation							Freq.Mono.(MHz)		Freq.Color(MHz)		Brightness [-255,255]	Hue [0°,360°]
Type	Vendor	Model	Sensor Model		Res.	FPS	Range	Opt.	Range	Opt.		
Analog CCTV	MingChuangDa	\	Sony	ICX811	976×582	50	53.2-57.6	55.6	67.6-71.1	69.2	-105∼133	360°
	ShunHuaLi	SHL-223		ICX811	976×582	50	44.7-51.7	48.1	43.1-44.6	43.5	-138∼156	360°
		SHL-019-1		ICX873	720×576	50	70.5-74.7	72.6	64.8-70.4	67.5	-124∼139	360°
	Szrs	\		Unknown	640×480	60	85.2-89.2	87.3	51.3-53.5	52.6	-110∼148	360°
	LantTian	TD-813		ICX663	976x582	60	47.4-48.7	47.9	57.3-59.8	58.0	-137∼145	360°
	Mintron	MTV-37S10P		ICX405	798×548	50	94.4-98.2	96.0	60.8-64.9	62.4	-116∼128	360°
		MTV-73X11HP		ICX409	798×548	50	97.2-99.1	98.2	67.2-69.1	68.4	-92∼117	360°
	KangShi	\		ICX811	976×582	60	56.5-57.2	56.7	57.3-63.4	60.9	-108∼131	360°
	Hayear	\		Unknown	1280×1024	60	81.5-86.0	83.7	74.3-77.1	75.6	-87∼114	360°
Digital Ethernet	Basler	ACA1300-30GC		ICX445	1296×966	60	\	\	59.5-67.2	63.6	-59∼64	360°
	MindVison	MV-UBD130C	Sharp	Unknown	1280×960	35	\	\	41.3-66.5	53.9	-46∼62	360°
		MV-GED130C		Unknown	1280×960	43	\	\	63.7-68.2	66.0	-55∼69	360°
		MV-UBD32C		Unknown	640×480	140	\	\	58.8-69.4	64.2	-88∼103	360°
	DaHeng	MER-032-120GC		RJ33B	656×492	120	48.3-76.6	62.3	81.7-100	92.8	-34∼41	360°
	Hikivision	MV-CE013-50GC		RJ33B4A	640×480	30	\	\	64.4-68.0	66.2	-37∼59	360°

Impact of Environment

Impact of Distance

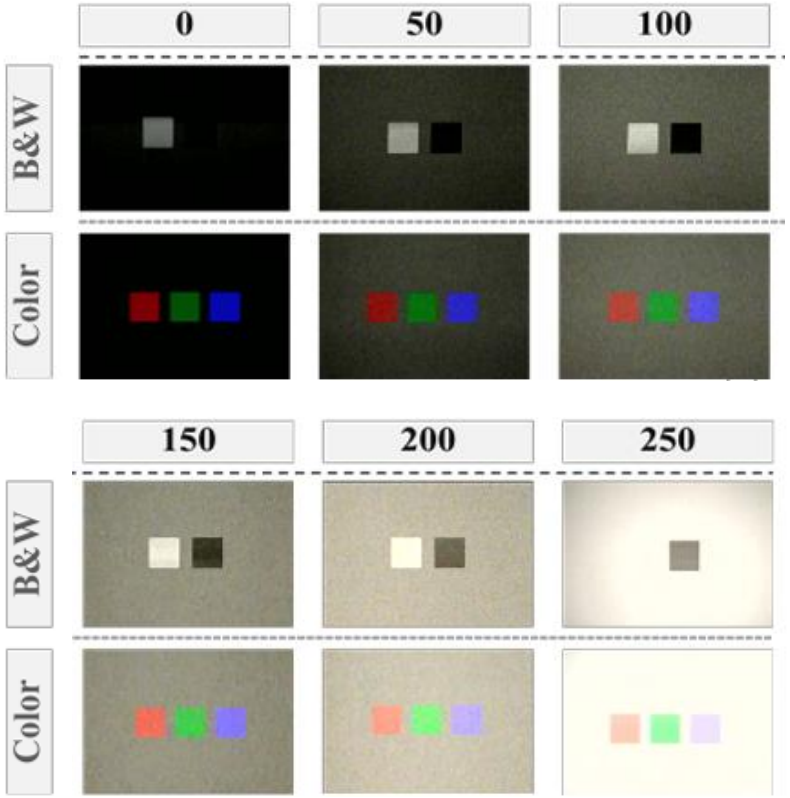


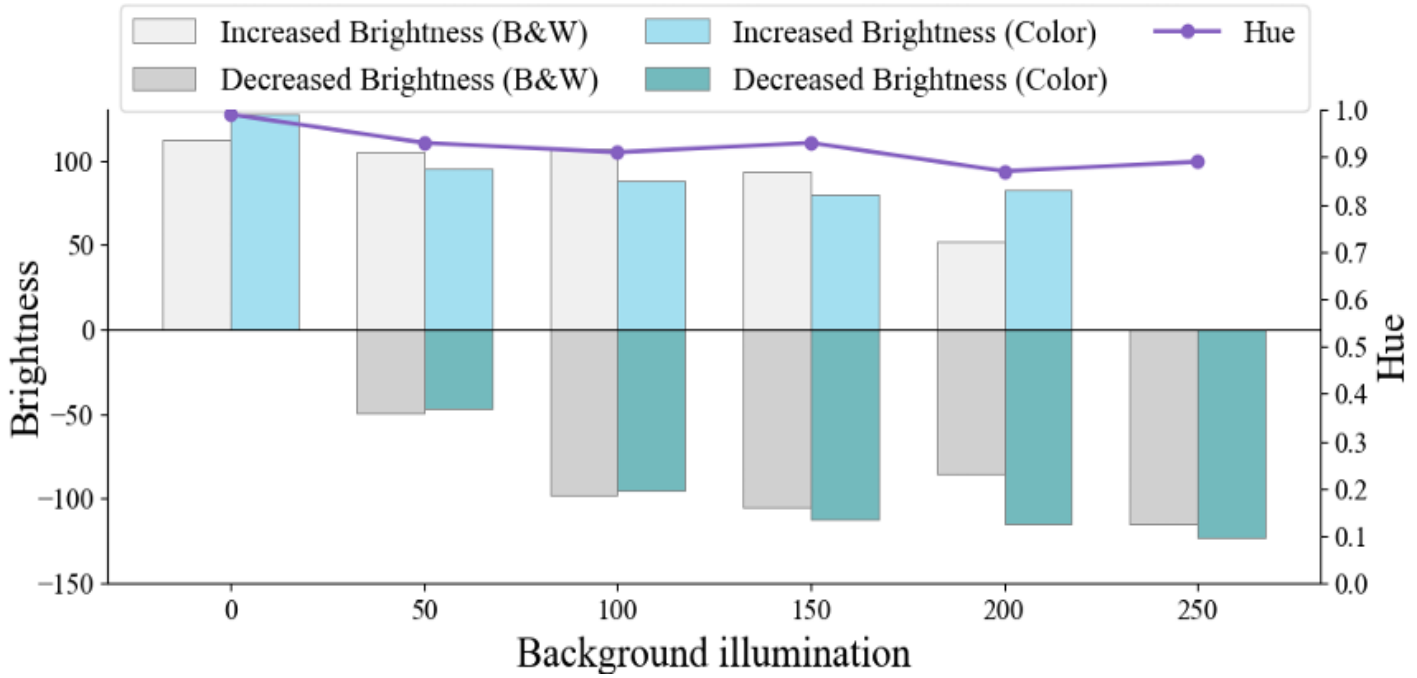
Impact of Angle



Injection is robust at different angles, with a 40cm attack distance.

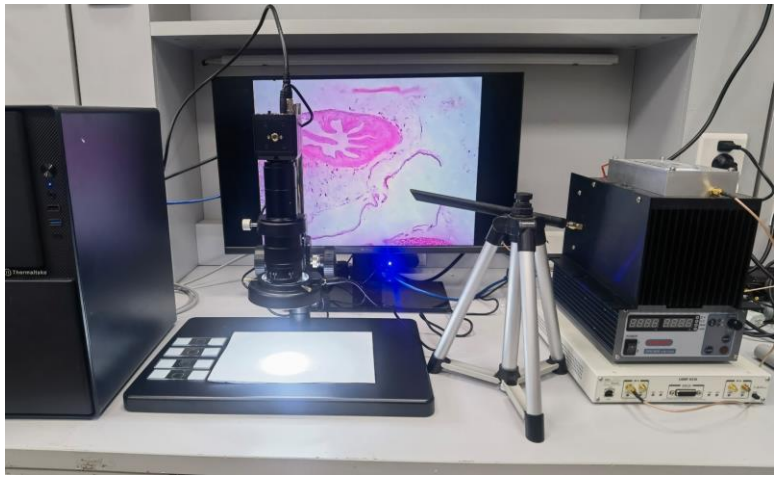
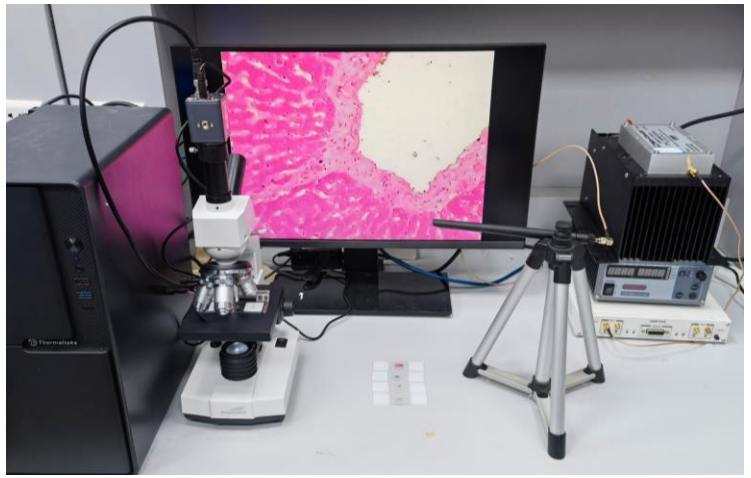
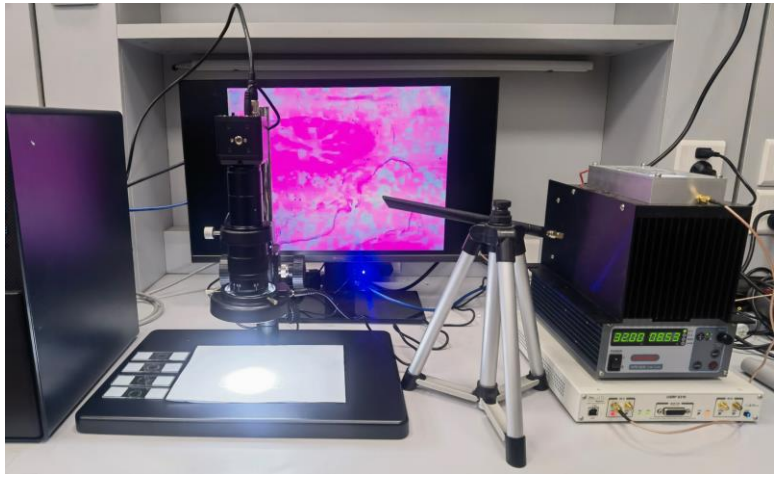
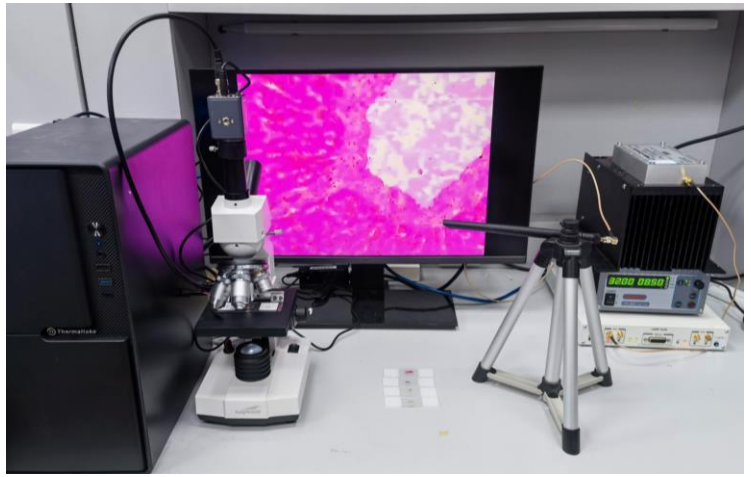
Impact of Ambient Brightness





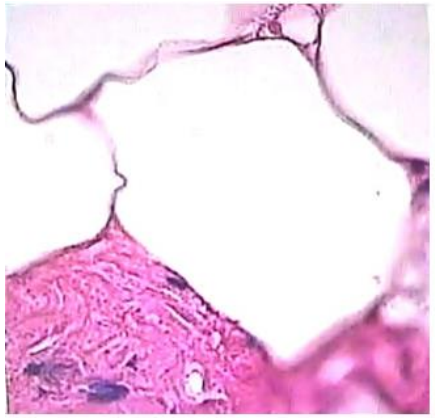
The injection exhibits robustness under various light conditions

Case Study 1: Medical Diagnosis

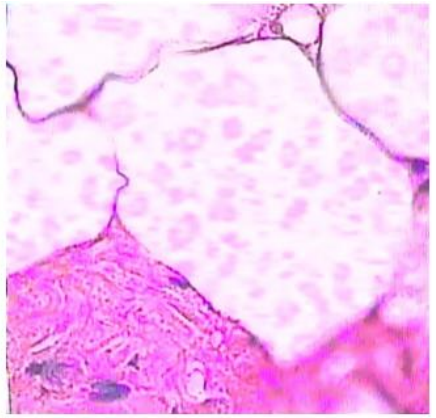
	Model-1: SHL-10A	**Model-2: SN-BP30**
Benign		
Attacked		

Case Study 1: Medical Diagnosis

Creation Attack

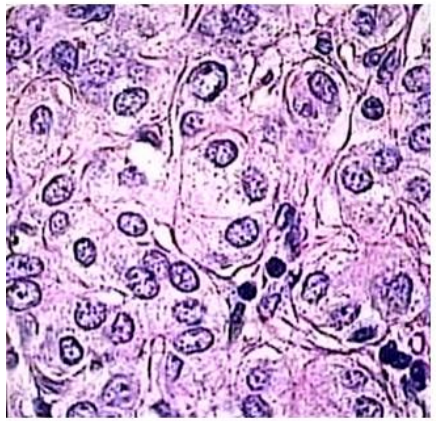


Ground Truth

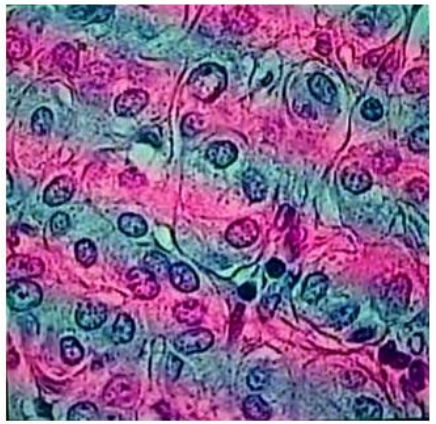


Creation Attack

Hiding Attack



Ground Truth



Hiding Attack

Evaluation Results

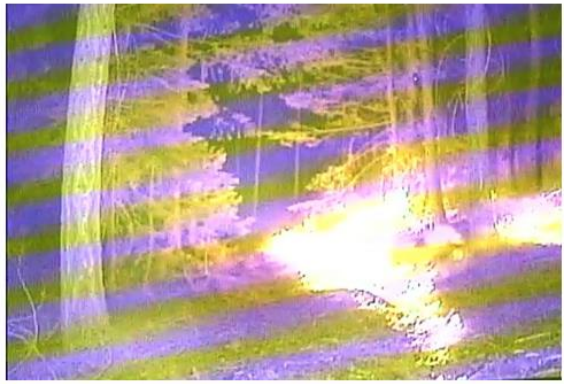
Dataset	Model	Status	Metrics			
			Precision	Recall	Accuracy	F1-Score
Camelyon16	DSMIL	Benign	0.68	0.59	0.66	0.63
		Attack	0.37	0.33	0.40	0.34

Case Study 2: Fire Detection

Ground Truth: non-fire

Creation Attack: fire, 0.77

Ground Truth: fire, 0.78



Hiding Attack: non-fire

Evaluation Results

Dataset	Model	Status	Metrics			
			Precision	Recall	Accuracy	F1-Score
NASA 2018	Yolov5	Benign	0.91	0.63	0.79	0.75
		Attack	0.09	0.08	0.15	0.09
	FireNet	Benign	0.94	0.58	0.77	0.72
		Attack	0.11	0.09	0.18	0.10
D-Fire	Yolov5	Benign	0.96	0.68	0.83	0.80
		Attack	0.14	0.11	0.21	0.12
	FireNet	Benign	0.93	0.65	0.80	0.76
		Attack	0.05	0.04	0.17	0.05

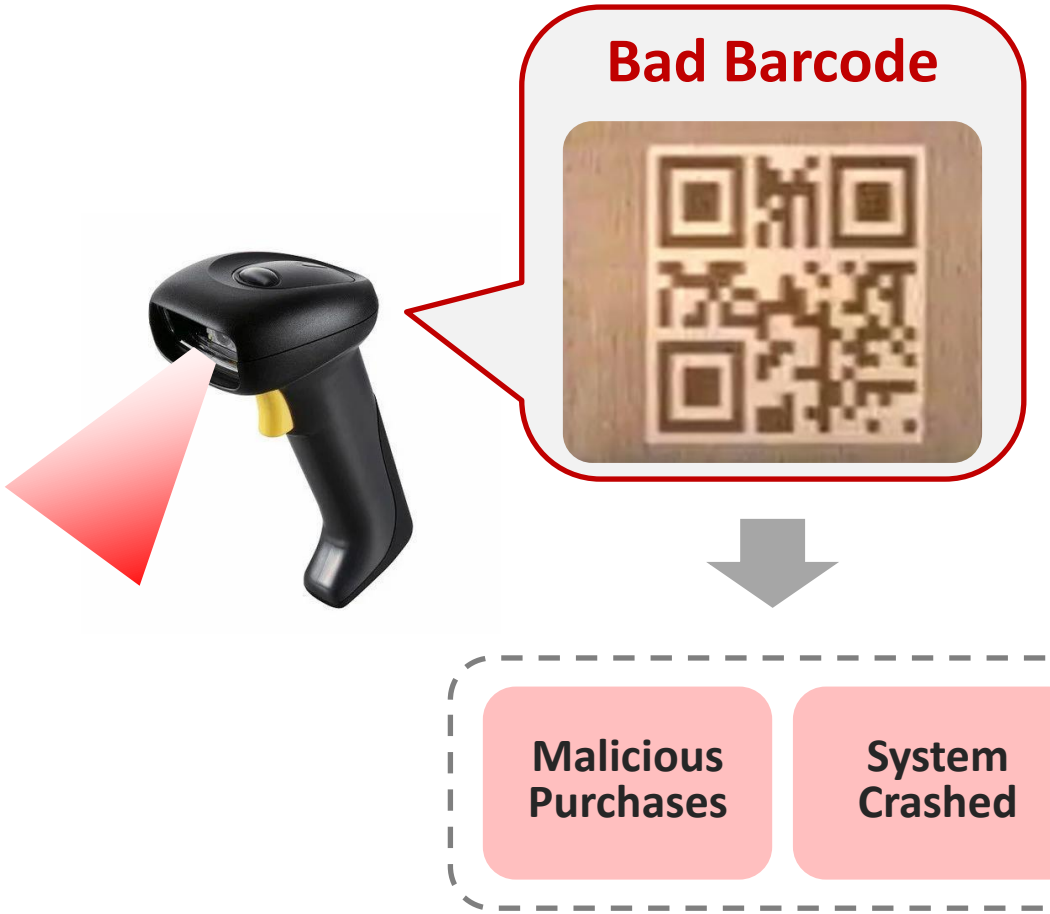
Case Study 3: QR Code Scanning

Ground Truth

Malicious Text

Malicious Picture

Malicious Script



Case Study 4: Night Vision Object Detection

Injected Persons

Injected Cars

The injection success rate was over 90% across 60 images.

Case Study 5: Deceit to the human

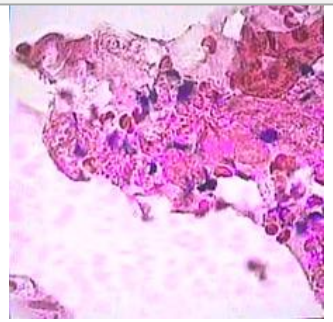
Attack images in User Study:

Text

Logo

Fire

Cell



QR code

Traffic

Results

False Positive Rate: 0.30

False Negative Rate: 0.54

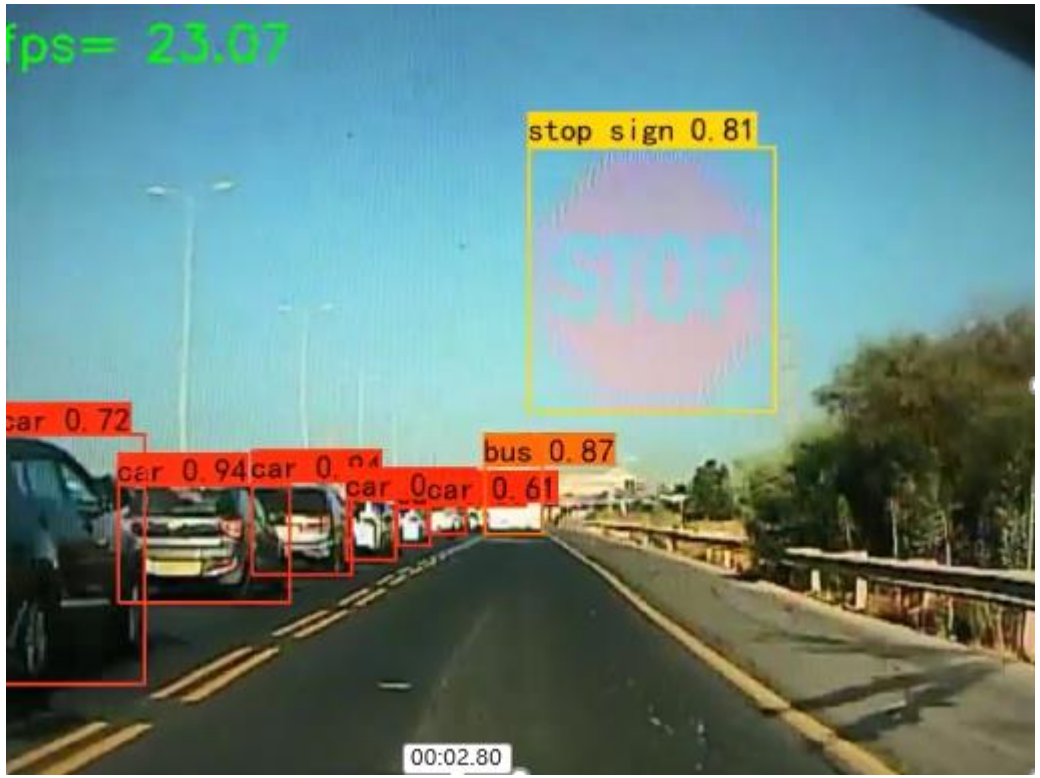
Accuracy: 0.58

*questionnaires on 40 users

Dynamic Injection

Demos can be found on *https://sites.google.com/view/ghostshot*

Demo-1



Demo-2

Countermeasures

- *Shield* CCD Cameras with specialized materials
- Apply the low-pass filters and Include redundancy pixels
- Apply image forgery detection

Conclusion

- *Design the attack against CCD cameras that can inject arbitrary monochrome or color images through IEMI.*

- Perform attack with 15 CCD cameras, demonstrated the threat of the attack to computer vision systems and the ability to mislead humans.

- Propose hardware and software methods to defend against the attack.

GhostShot: Manipulating the Image of CCD Cameras with Electromagnetic Interference

Thanks for listening! Q&A





Yanze Ren

yzren@zju.edu.cn

USSLAB

Paper

Demo

Synchronization From EMI Leakage