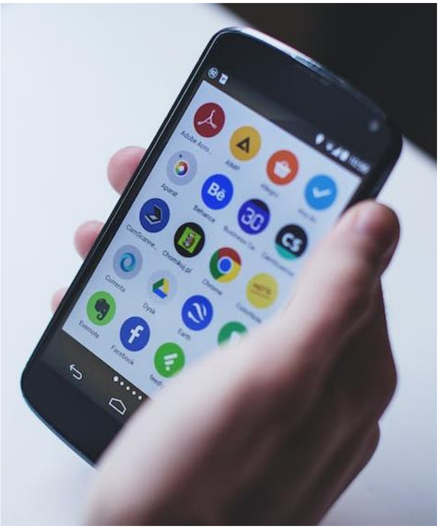
Spoofing Real-world Face Authentication Systems through Optical Synthesis

Yueli Yan, Zhice Yang

上海科技大学
ShanghaiTech University

Using Face for Authentication



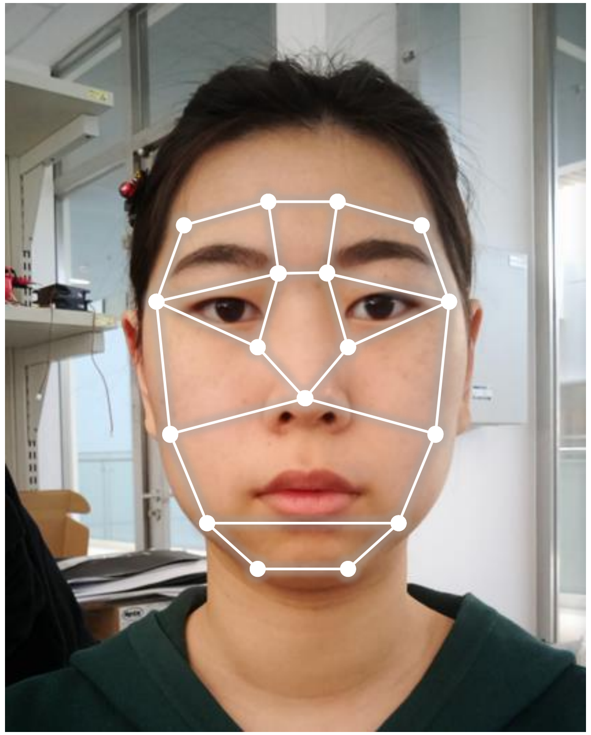
Screen Lock

Door Access

Payment

Photo Sources: Yueli Yan, and pexels.com with CC license

Using Face for Authentication



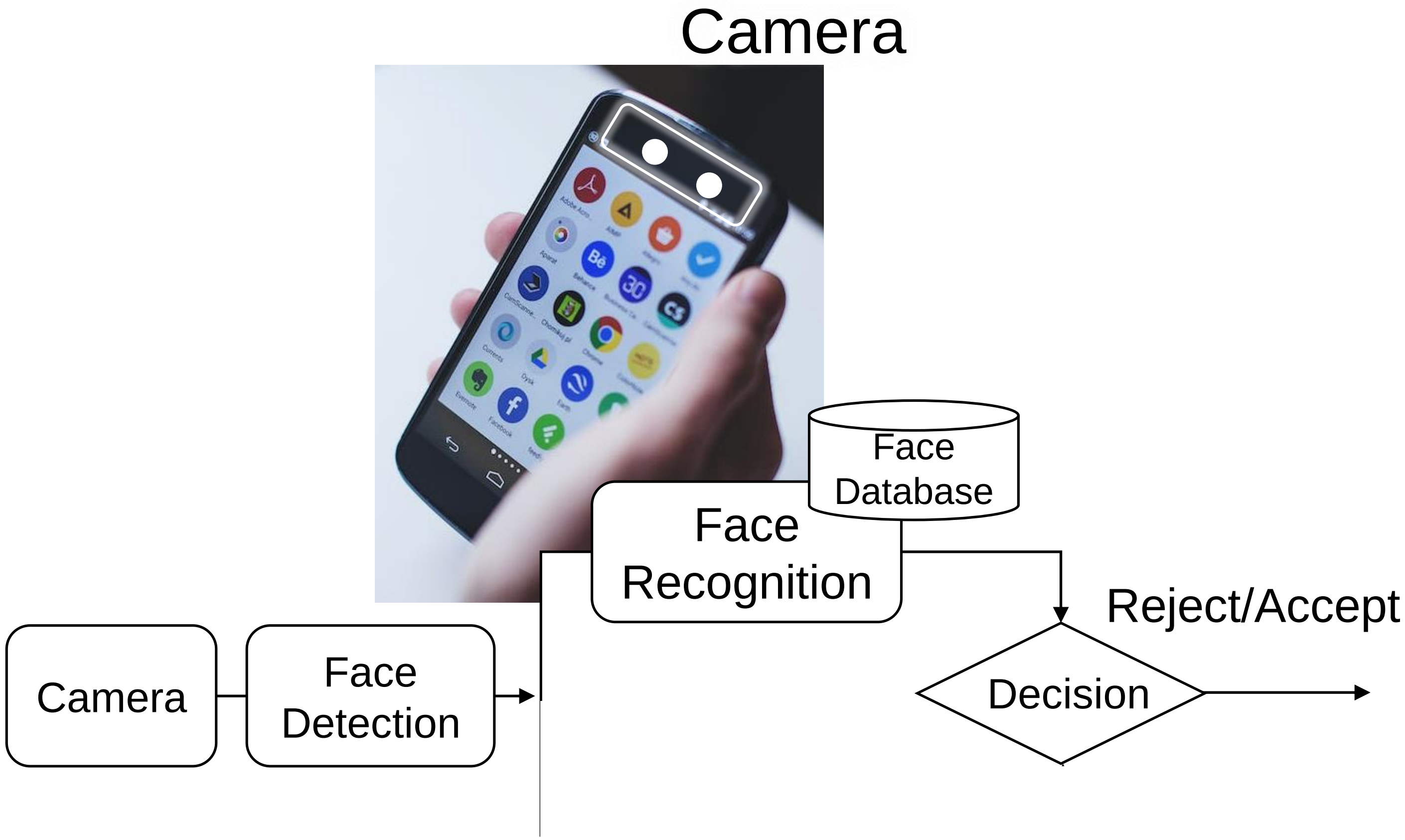


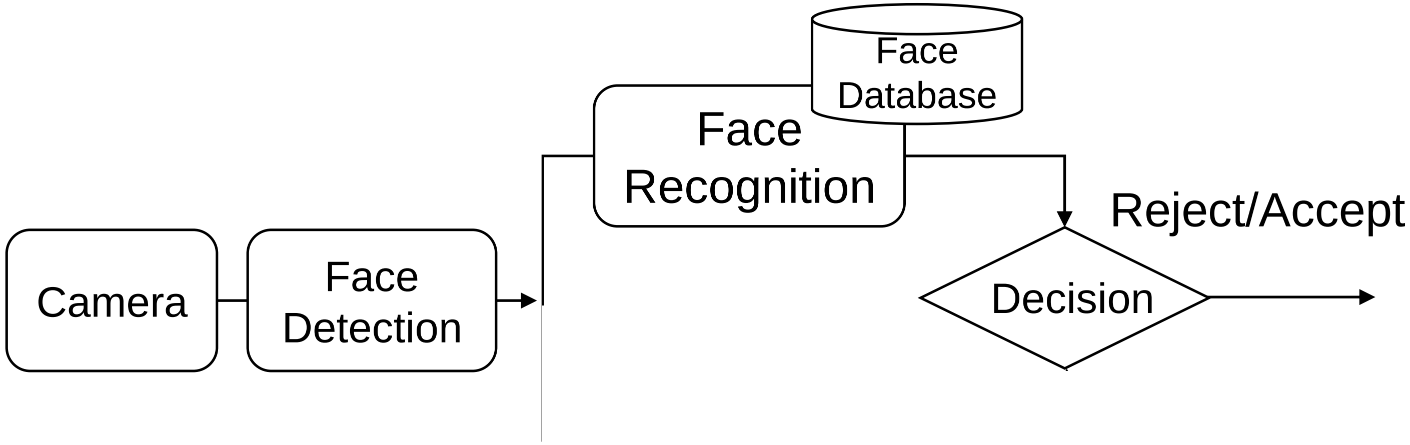
Photo Sources: Yueli Yan, and pexels.com with CC license

Anti-spoofing Methods

- Dynamic Method
  - Record a video
  - Large latency
  - General RGB camera

➢ Static Method
  - Take single-shot images
  - Low latency
  - Multimodal camera

Display a Photo ?



Face Database

Face Recognition

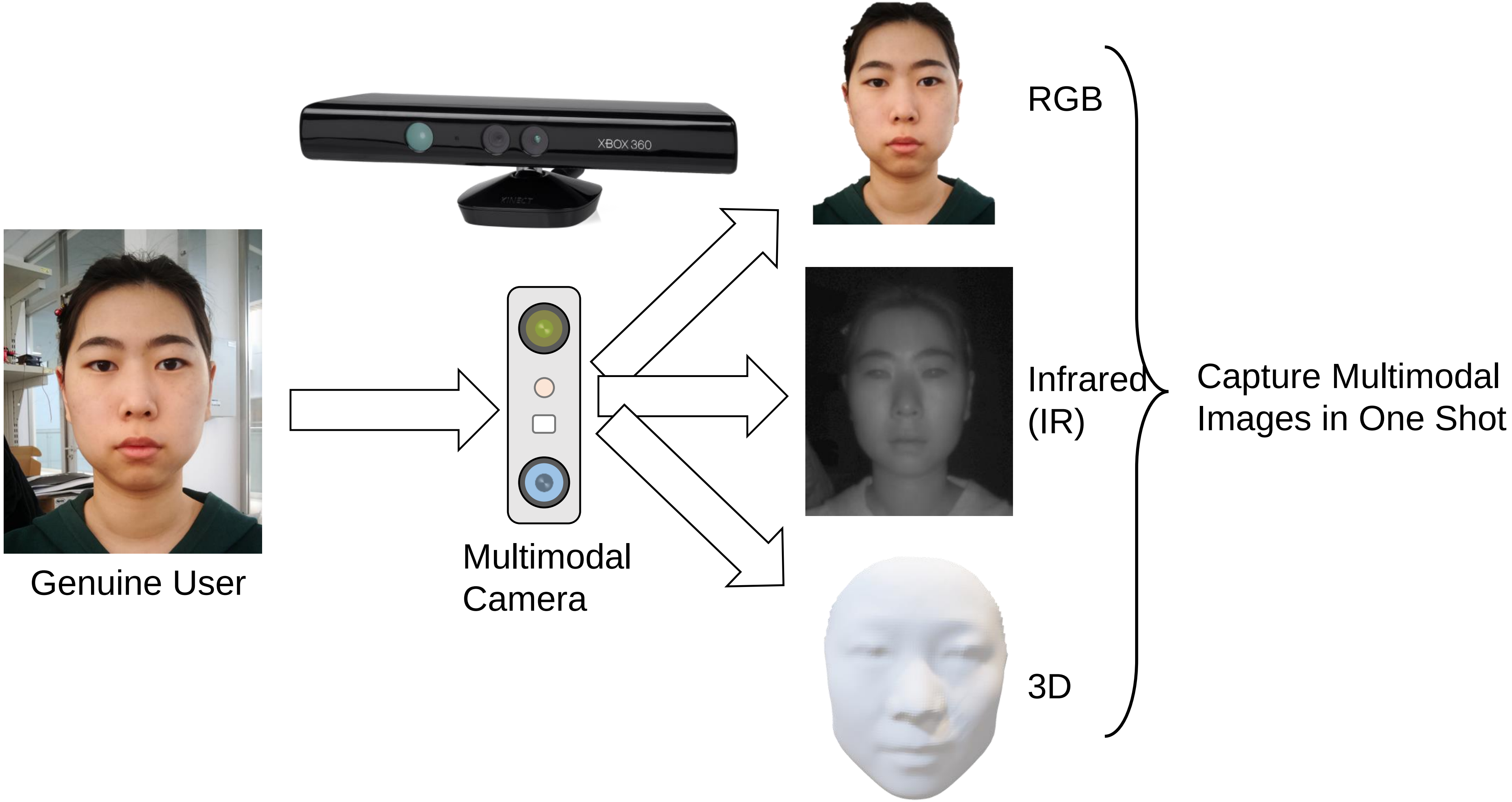
Reject/Accept

Camera

Face Detection

Decision

Multimodal Camera



Genuine User

Multimodal Camera

RGB

Infrared (IR)

3D

Capture Multimodal Images in One Shot

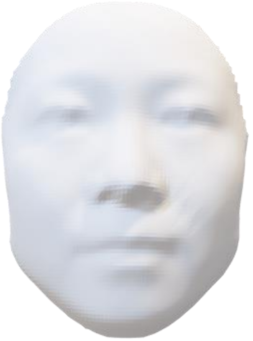
Spoofing Multimodal Cameras ?

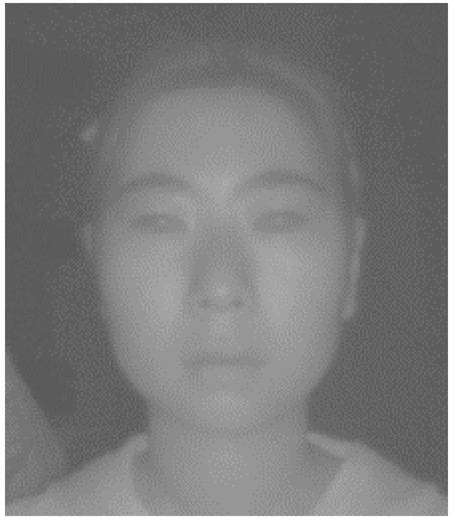
- 2D Attacks
    - No 3D facial features
- 3D Head Model
    - Expensive
    - Cannot simultaneously present IR and RGB modalities

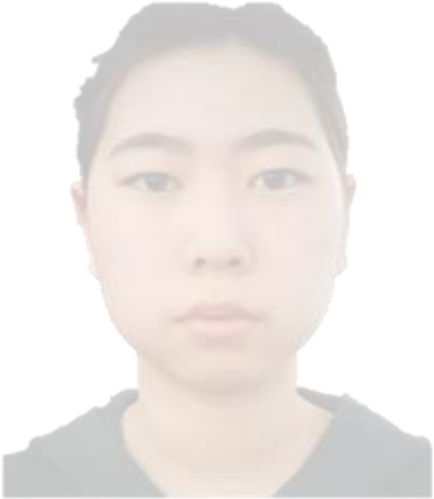
A questionable basis of current static anti-spoofing: no effective way to simultaneously present multiple modalities

Hua-pi Attack

- Try to Present Multimodal Images Simultaneously

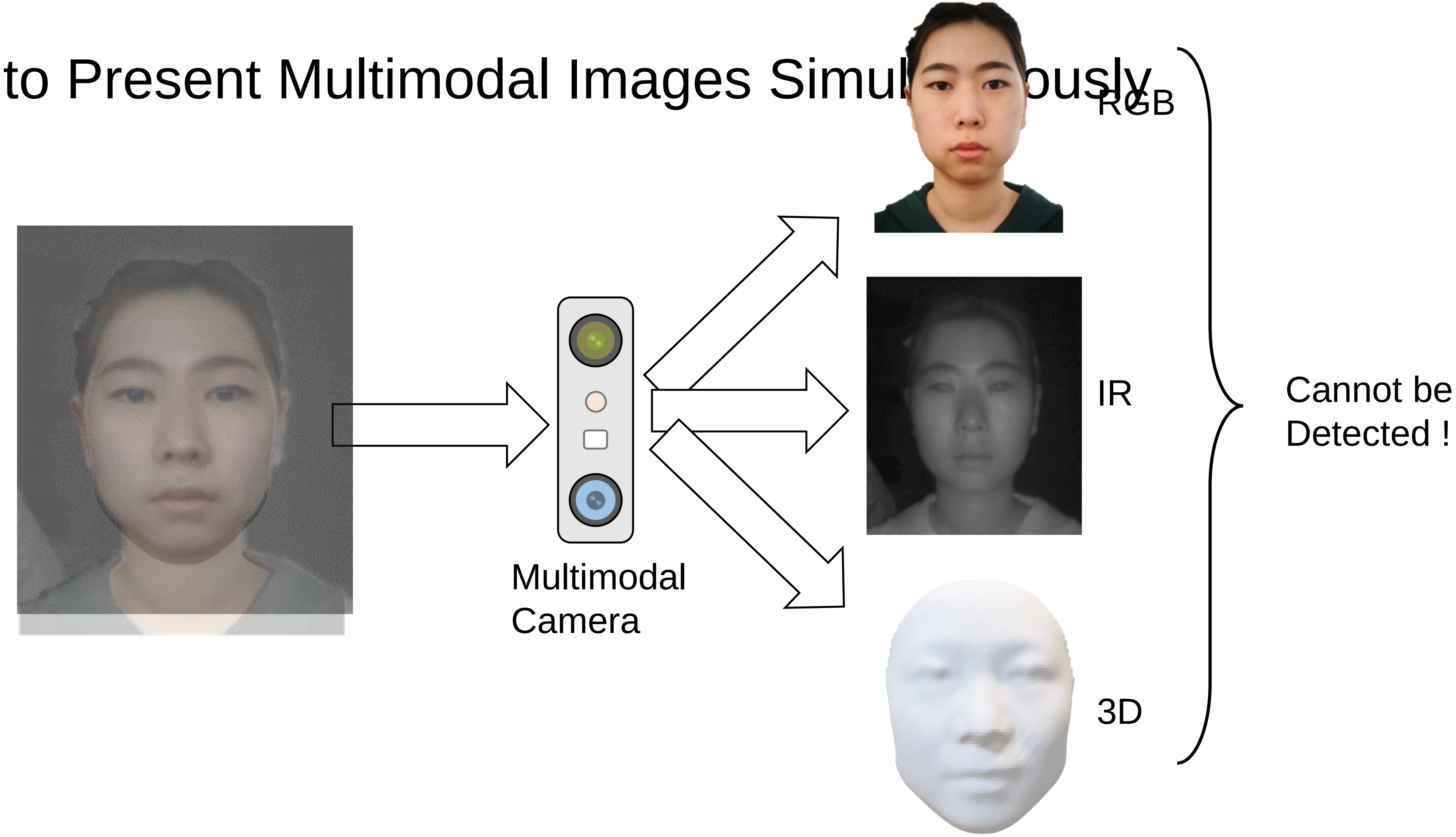




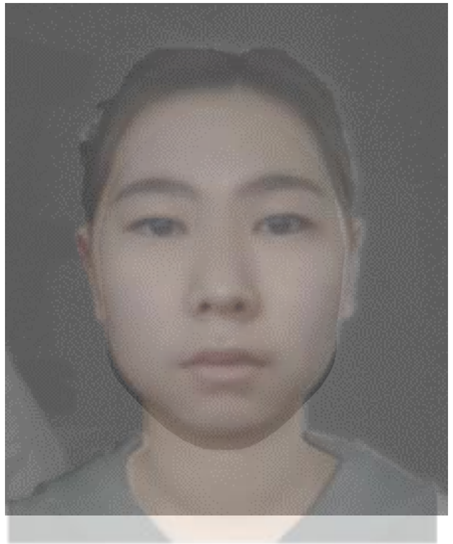


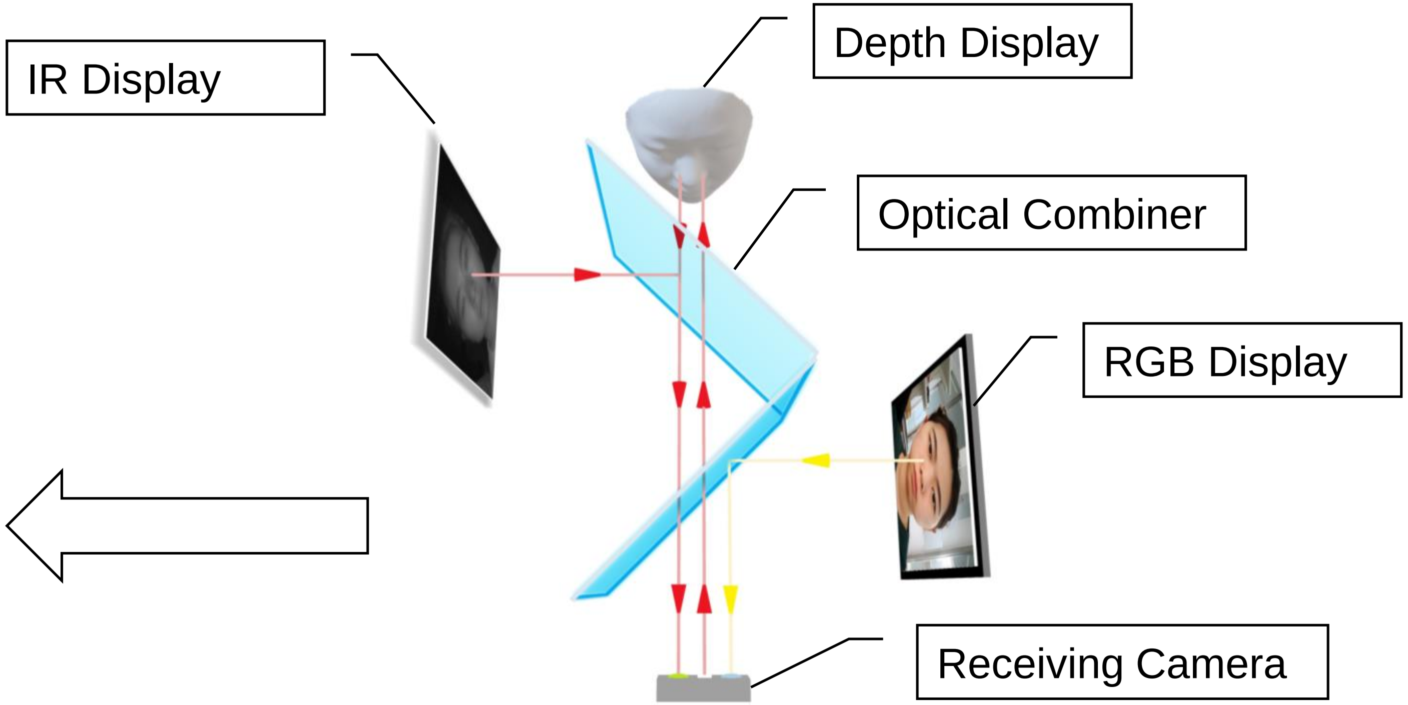
Hua-pi Attack

- Try to Present Multimodal Images Simultaneously



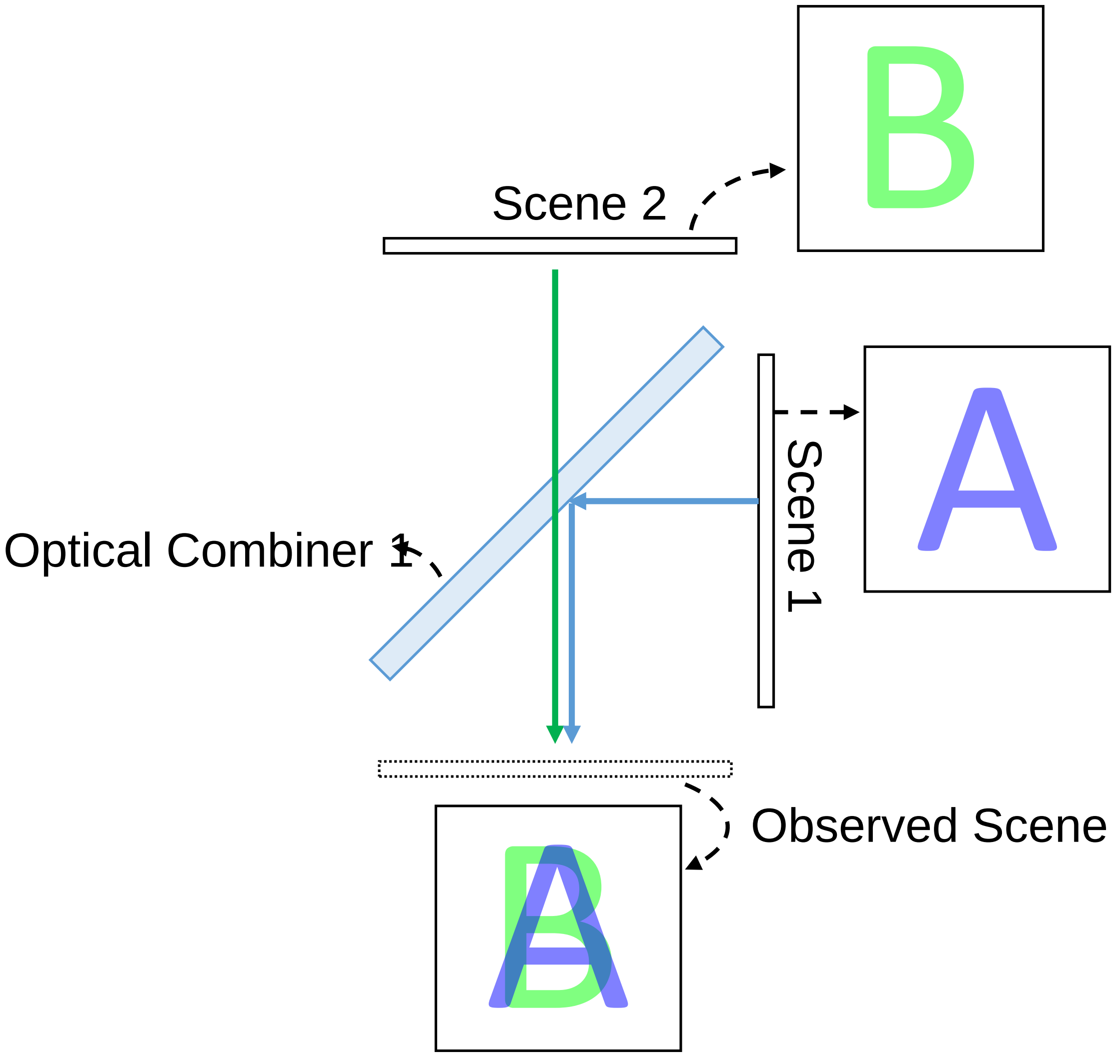
Hua-pi Display



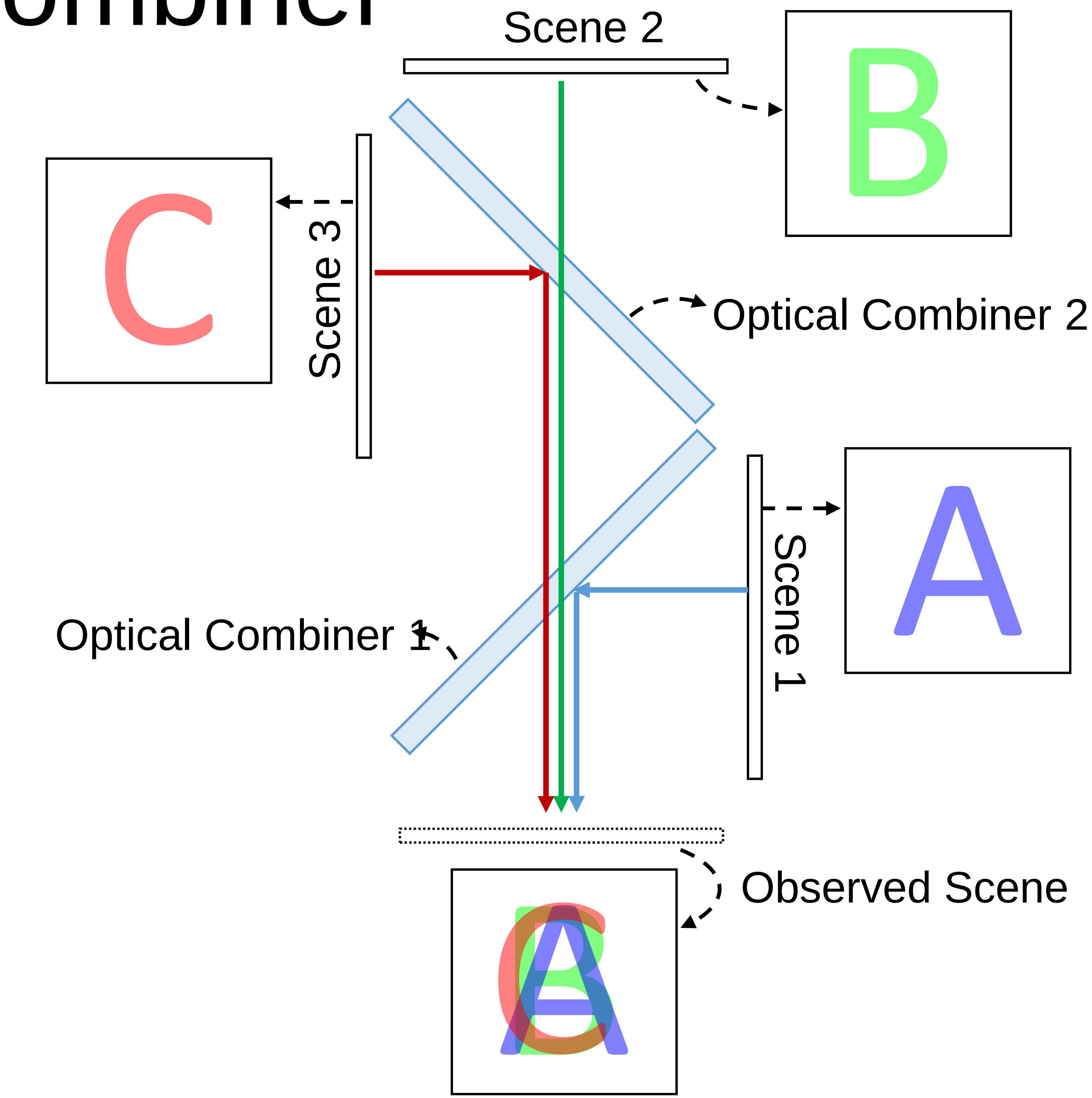


Hua-pi Display

Optical Combiner

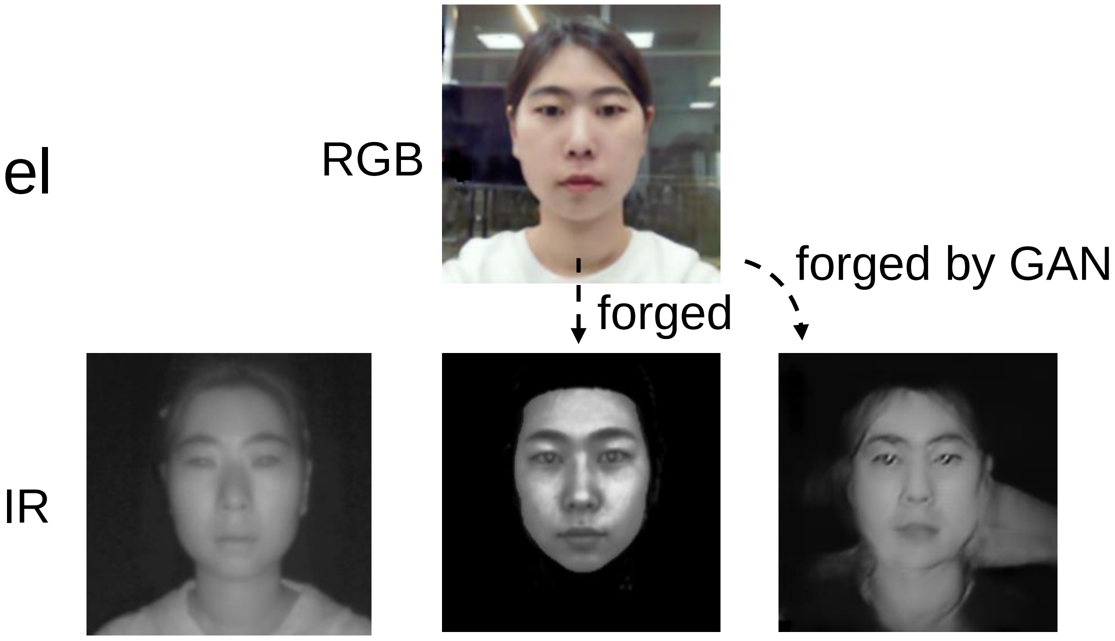


Optical Combiner



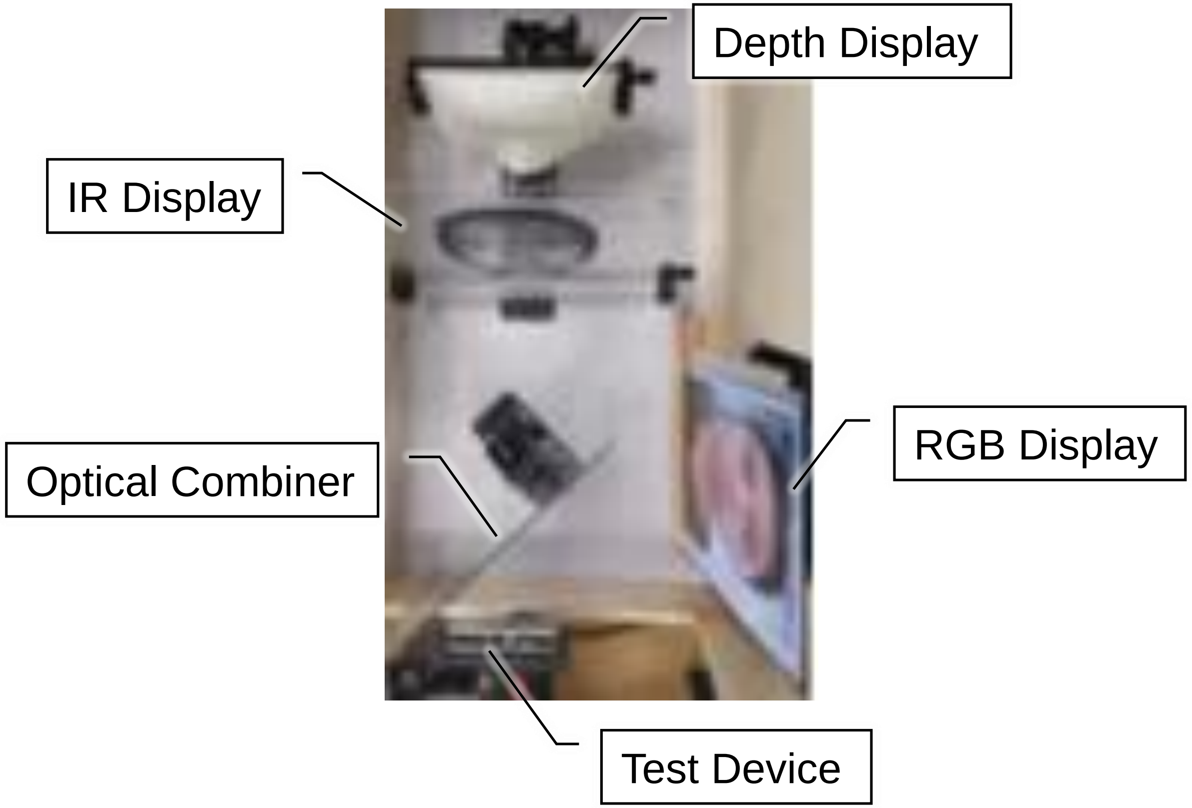
Display Modules for Different Modalities

- RGB Display
  - Hardware: high-resolution RGB panel
  - Content: public RGB photos
- IR Display
  - Hardware: laser-printed paper
  - Content: real or forged IR photos
- Depth Display
  - Hardware: more on paper
  - Content: physical 3D facial model
    - not necessarily from the same person



Results

- *Hua-pi* Display Prototype



Depth Display

IR Display

RGB Display

Optical Combiner

Test Device

- Cost
  - Hardware:
    - ~ U.S.$ 500
  - Per-attack Consumables:
    - < U.S.$ 1

Results

- 16 COTS devices from leading product vendors
- 20 participants of different age and ethnicity groups
- 80% pass rate

Tech.	Type	Vendor	Model	Modality	Algorithm
RGB+IR	Camera	Dumu	C2	RGB+IR	SDK1
		Dumu	C2	RGB+IR	SDK2
	Module	Dumu	C2	RGB+IR	built-in
		□□□	□□□	RGB+IR	built-in
		NXP	SLN-VIZNAS-IOT	RGB+IR	built-in
		Intel	RealSense F455	RGB+IR	built-in
	Product	□□□	(door access)	RGB+IR	built-in
Structured Light	Camera	Orbbec	Petrel	RGB +D$^{\wedge}$	SDK1
	Module	□□□	□□□	IR+D	built-in
		NXP	SLN-VIZN3D-IOT	IR+D	built-in
	Product	□□□	□□□	RGB+IR+D	SDK3
		□□□	(smartphone)	IR+D	built-in
		□□□	(smartphone)	IR+D	built-in
ToF	Camera	Sunny$^{\#}$	Mars05b	RGB+IR+D	SDK1
				RGB+IR	
				RGB +D	
				IR	
				RGB	
	Module	□□□$^{\#\#}$	□□□	IR+D	built-in
	Product	□□□	(smartlock)*	IR+D	built-in

Other Interesting and Important Results

- Available modalities are not all in use for anti-spoofing
  - *e.g.*, RGB camera is only for monitoring
- Cross-modality consistency is not verified
  - *e.g.*, RGB and IR photos could be from different persons
- The use of depth information is superficial
  - *e.g.*, one 3D head model passes all tests

Summary

- Consistent Effectiveness against Commercial Devices
- Low-cost
- Physical
- Blackbox

Thank You !

Contact: Zhice Yang yangzhc@shanghaitech.edu.cn