Virtual U: Defeating Face Liveness Detection by Building Virtual Models From Your Public Photos

Yi Xu, True Price, Jan-Michael Frahm, and Fabian Monrose

Department of Computer Science, University of North Carolina at Chapel Hill

USENIX Security

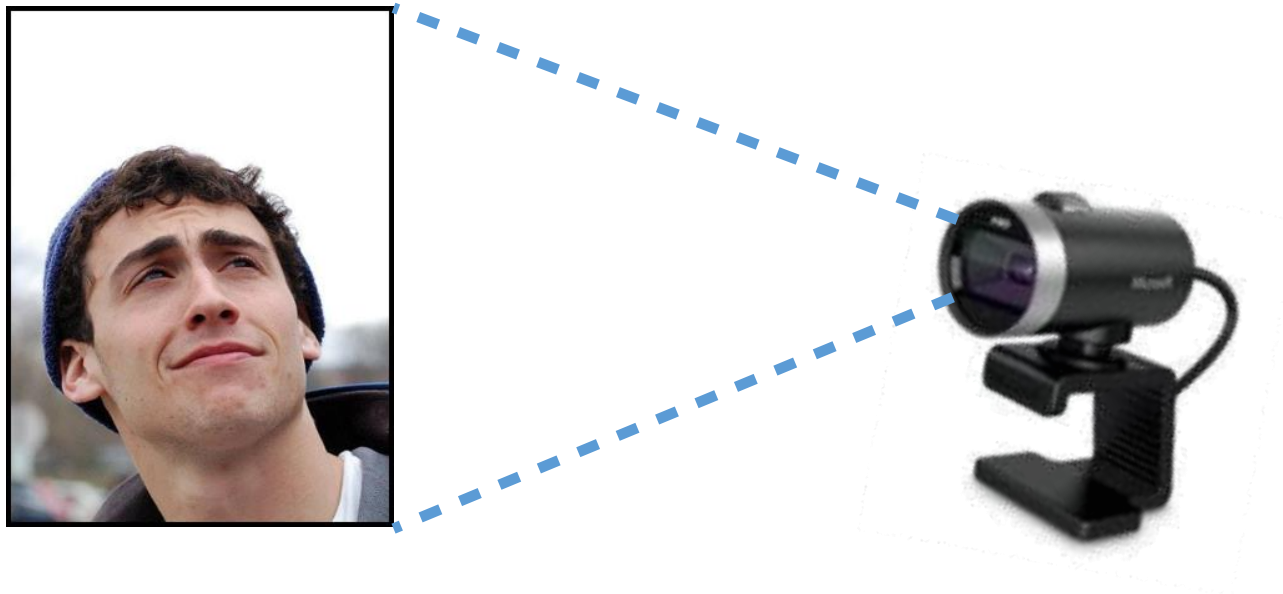
August 11, 2016

Face Authentication: Convenient Security

image source

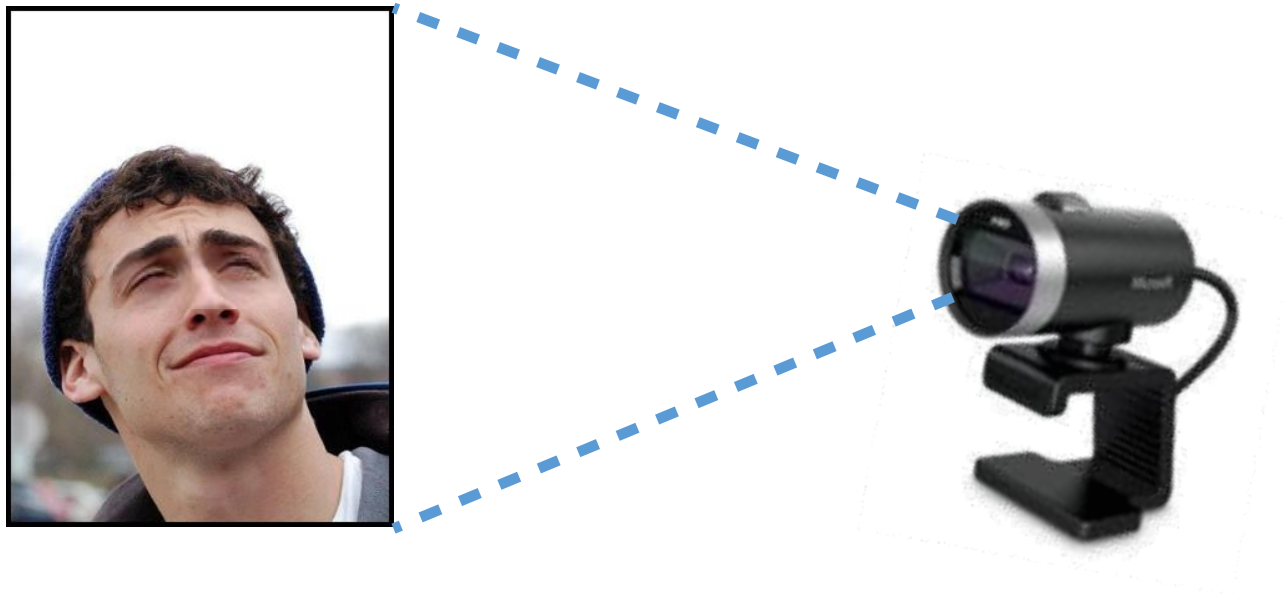
Evolution of Adversarial Models

- Attack: Still-image Spoofing



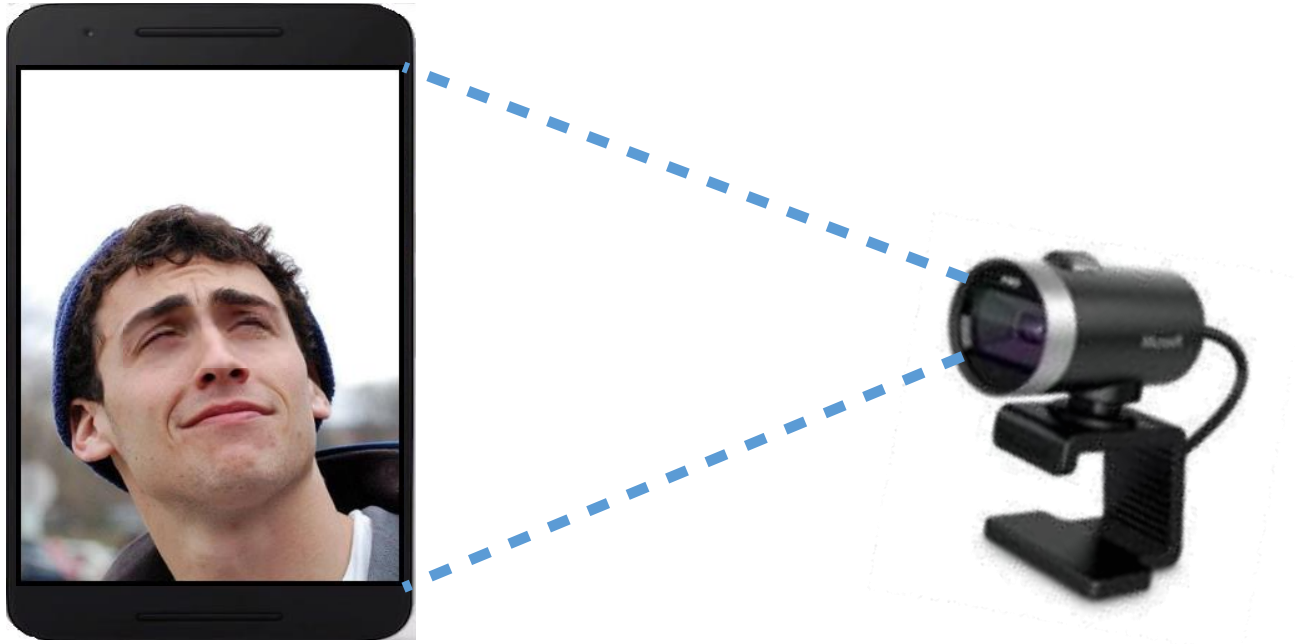
Evolution of Adversarial Models

- Attack: Still-image Spoofing
- Defense: Liveness Detection



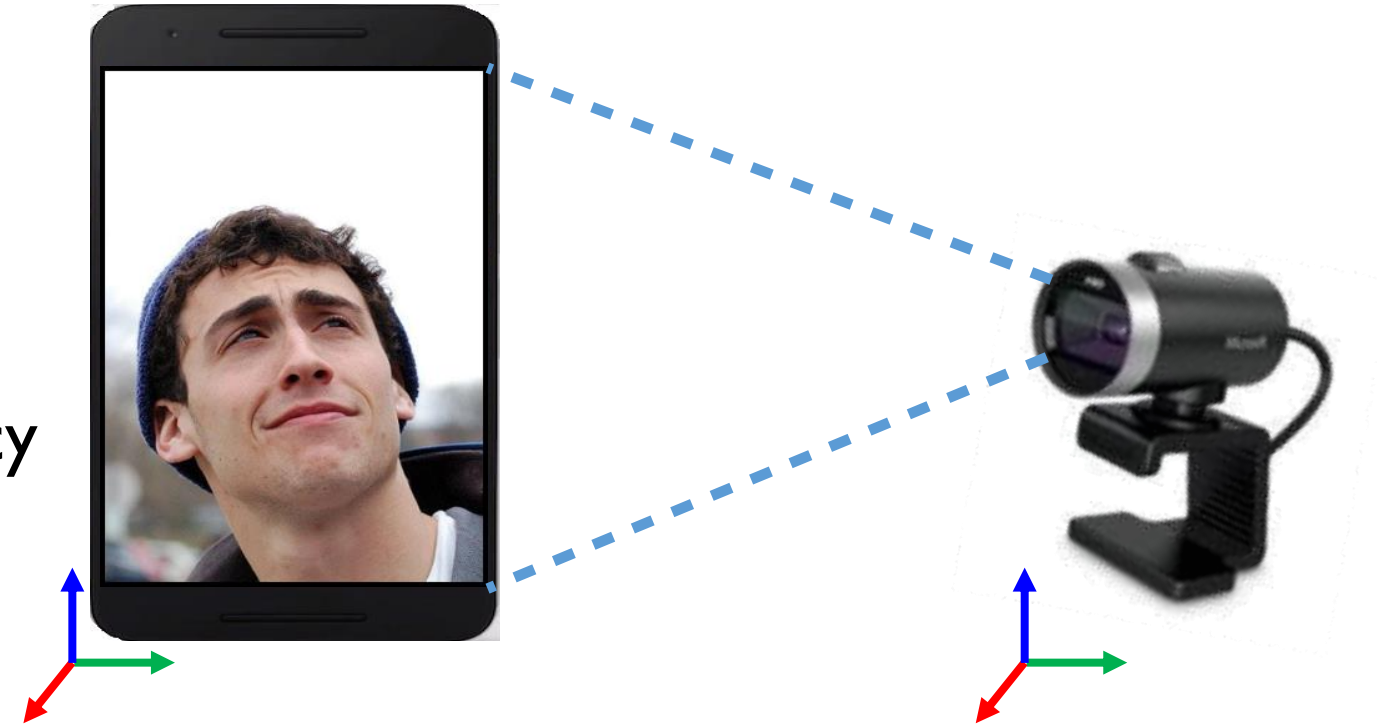
Evolution of Adversarial Models

- Attack: Still-image Spoofing
- Defense: Liveness Detection
- Attack: Video Spoofing



Evolution of Adversarial Models

- Attack: Still-image Spoofing
- Defense: Liveness Detection
- Attack: Video Spoofing
- Defense: Motion Consistency



Evolution of Adversarial Models

- Attack: Still-image Spoofing
- Defense: Liveness Detection
- Attack: Video Spoofing
- Defense: Motion Consistency
- Attack: 3D-Printed Masks

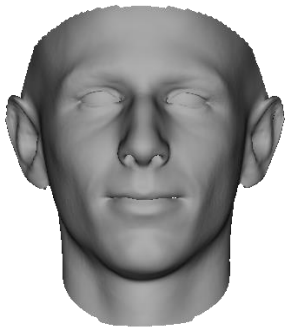
Virtual U: A New Attack

We introduce a new VR-based attack on face authentication systems solely using publicly available photos of the victim

Virtual U: A New Attack

1

2



3

4

Input Web Photos

Landmark Extraction

3D Model Reconstruction

Image-based Texturing

Gaze Correction

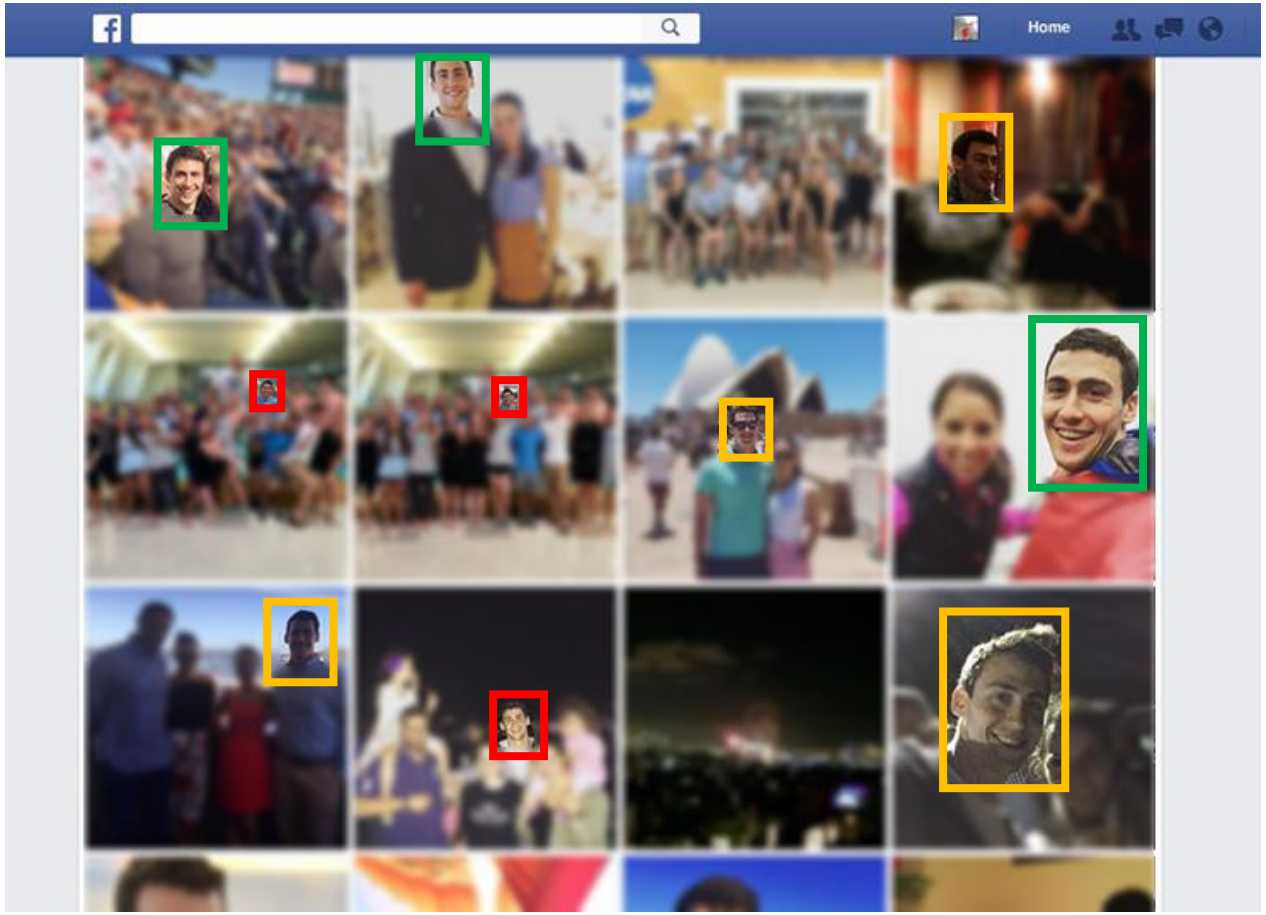
5

6

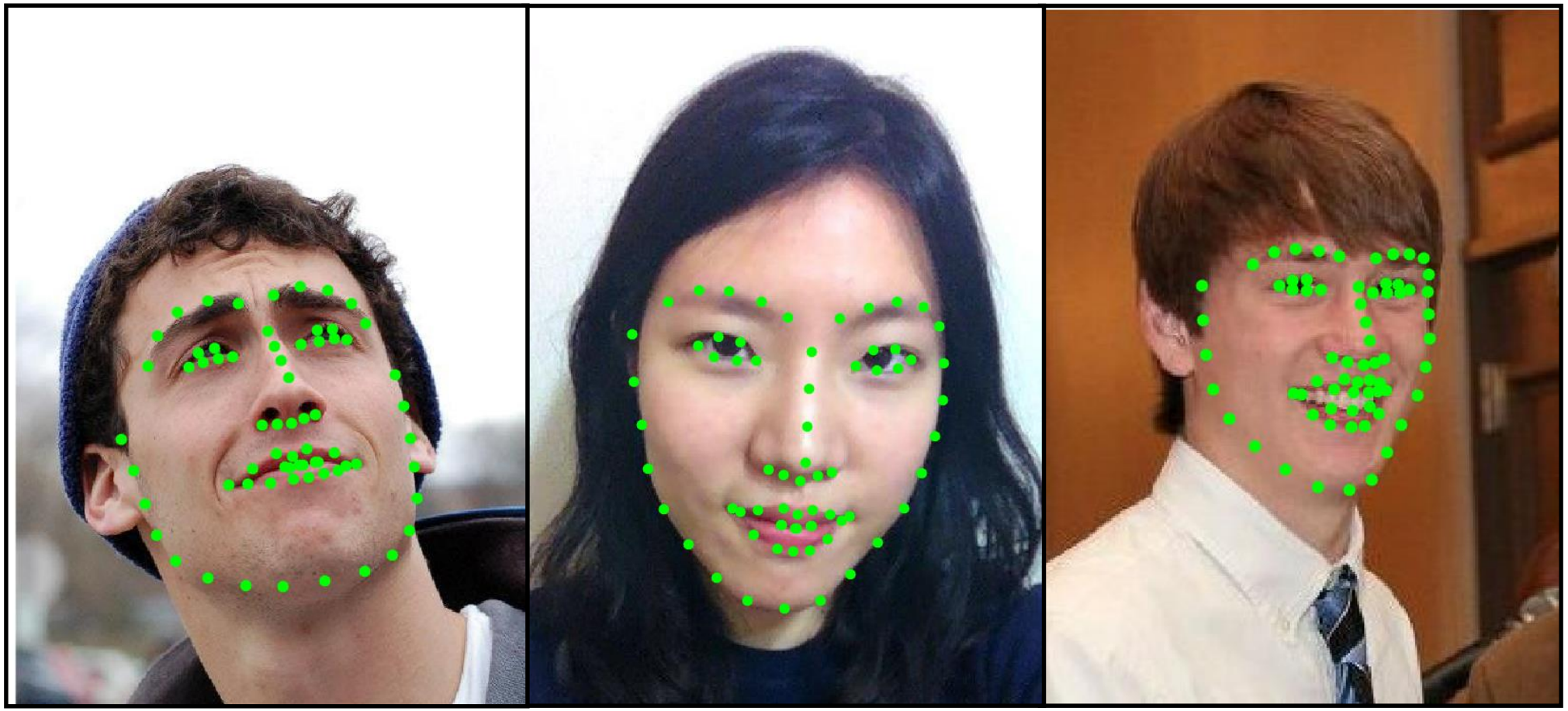
Expression Animation

Viewing with Virtual Reality System

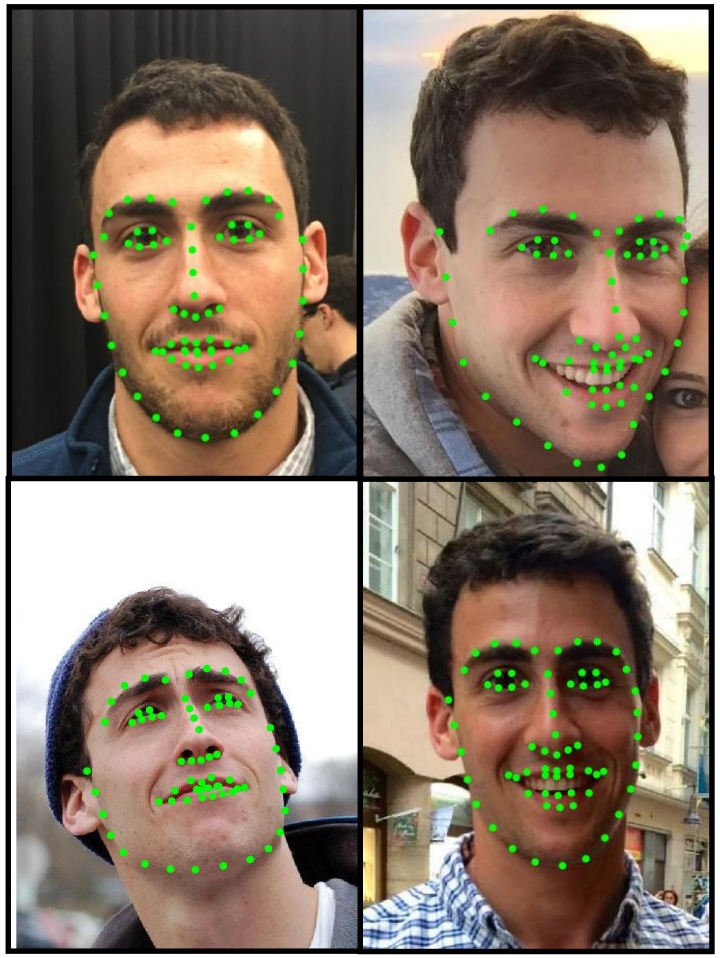
Leveraging Social Media

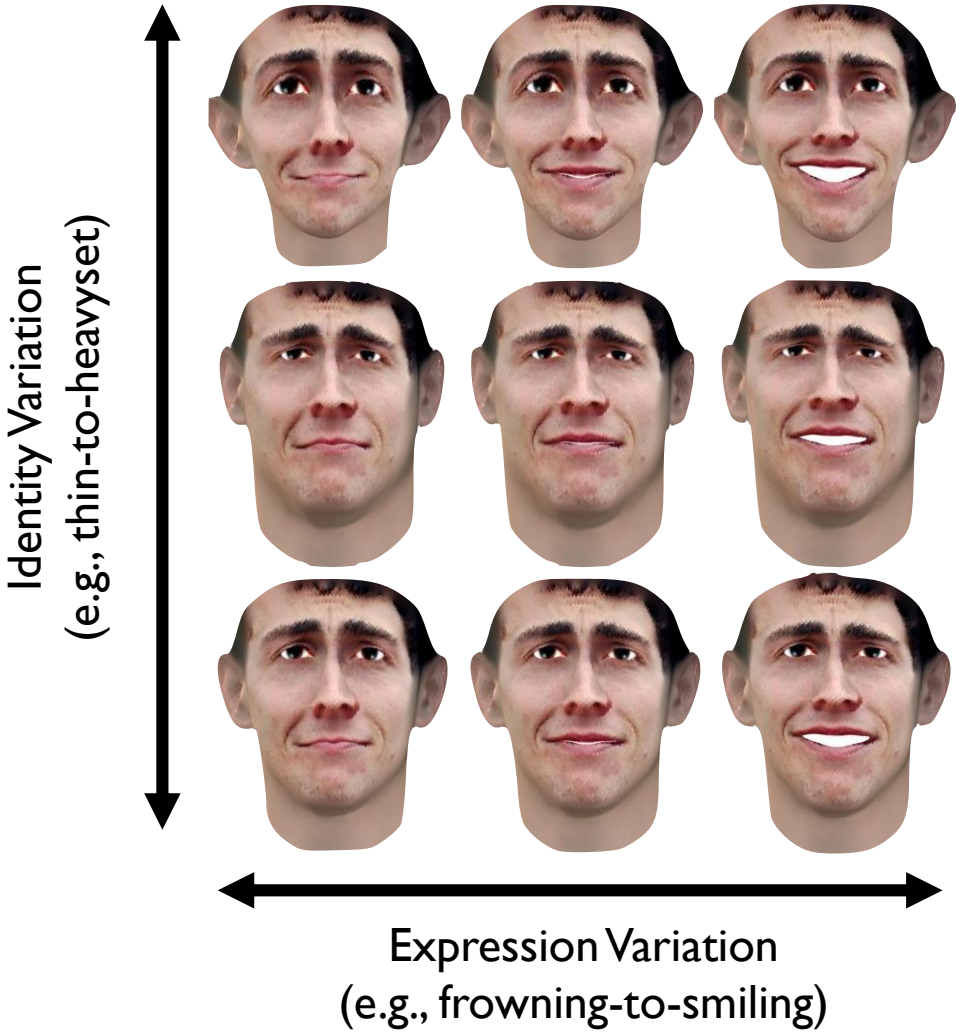


Landmark Extraction



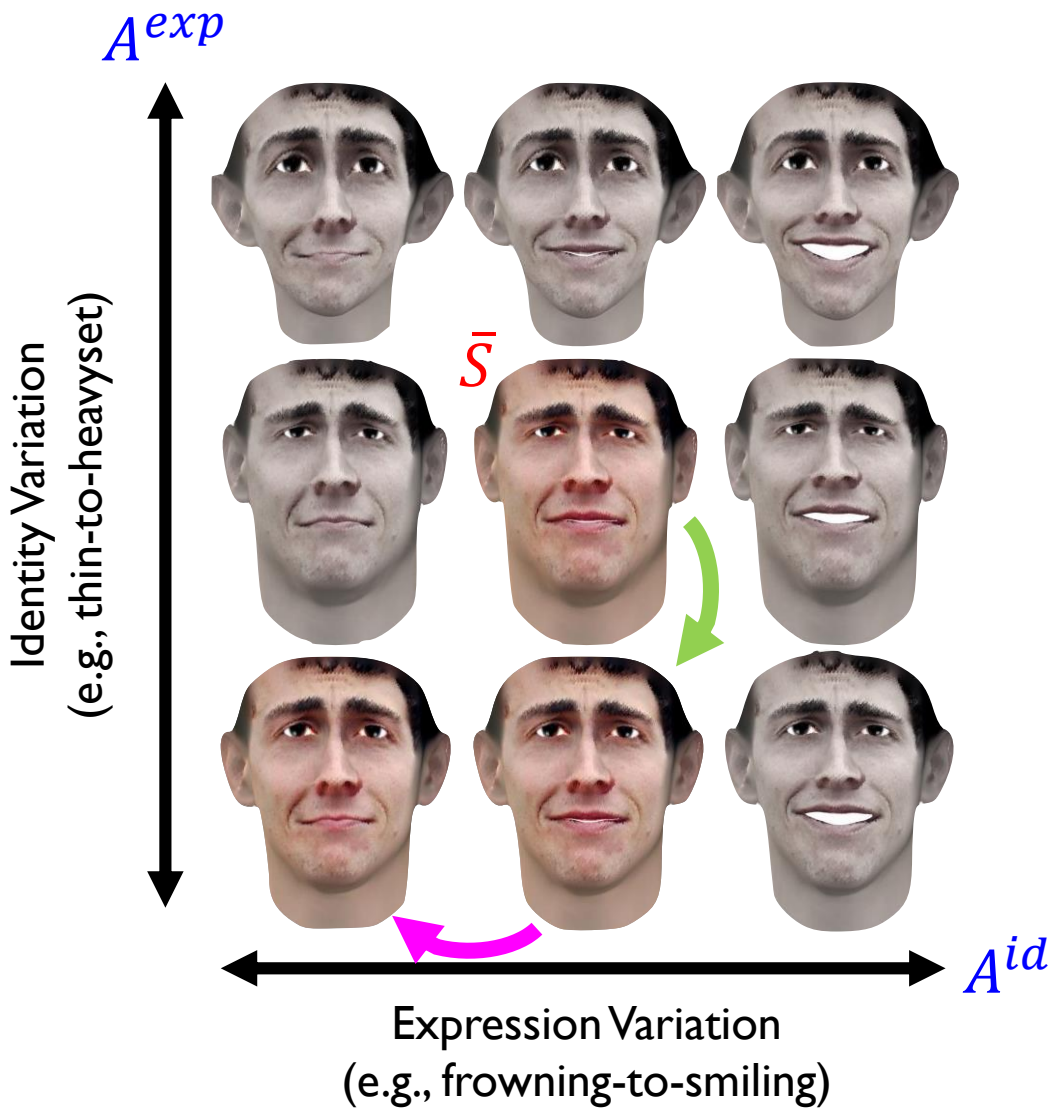
3D Face Model





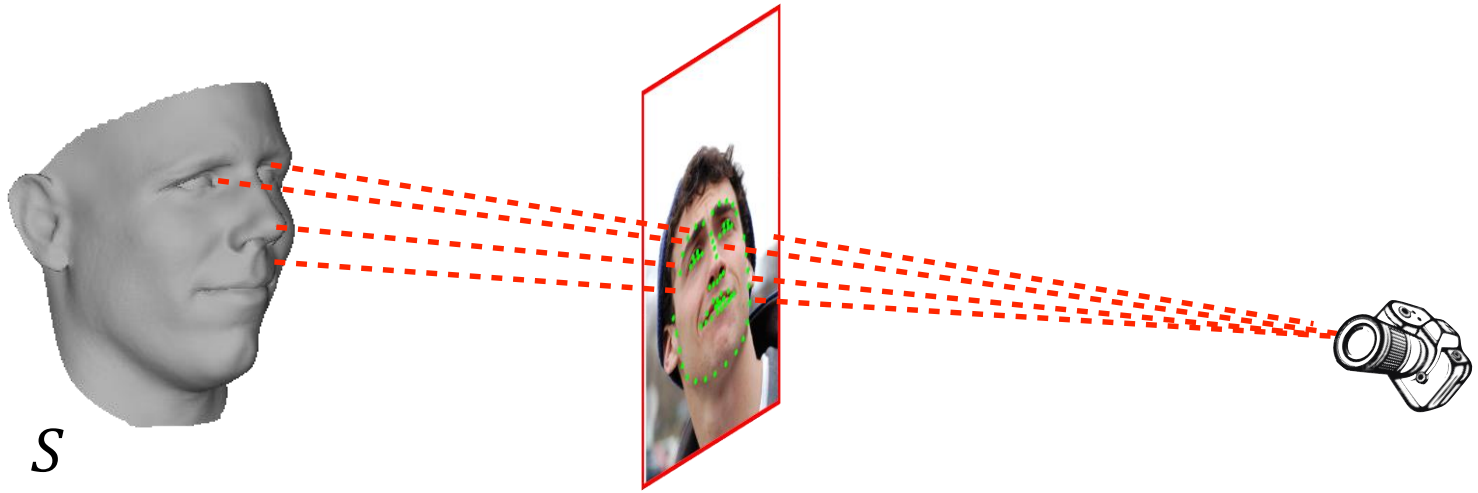
3D Face Model

$$S = \bar{S} + A^{id}\alpha^{id} + A^{exp}\alpha^{exp}$$



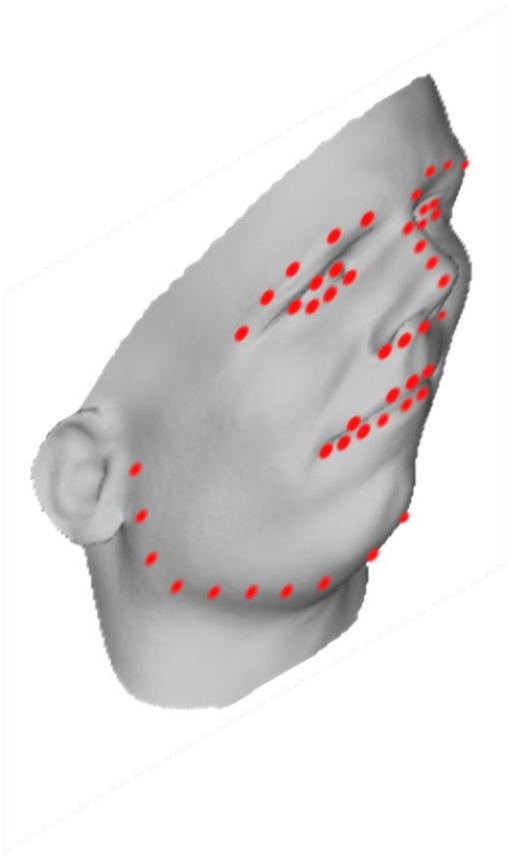
3D Face Model

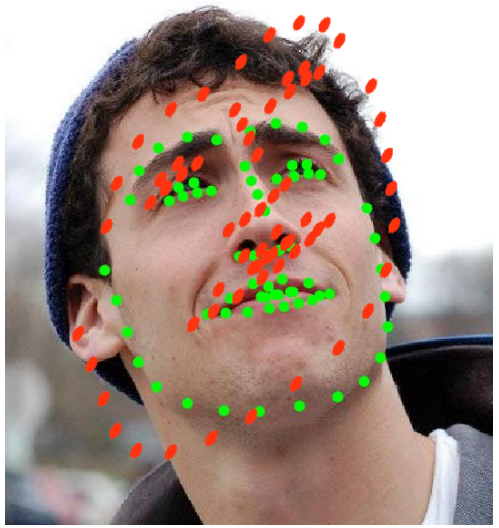
$$S = \bar{S} + A^{id}\alpha^{id} + A^{exp}\alpha^{exp}$$



3D Face Model

$$S = \bar{S} + A^{id}\alpha^{id} + A^{exp}\alpha^{exp}$$





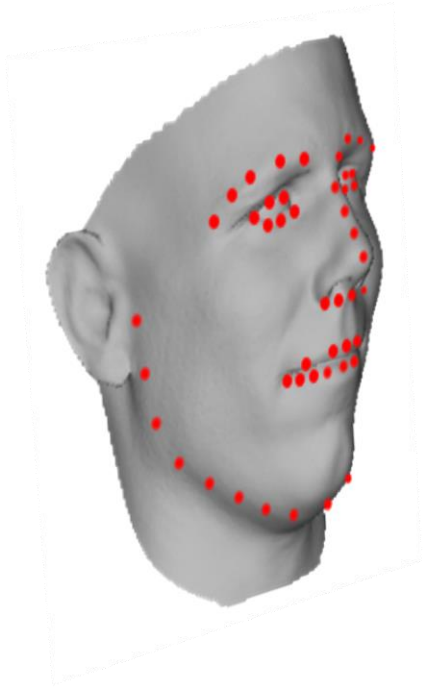
Pose

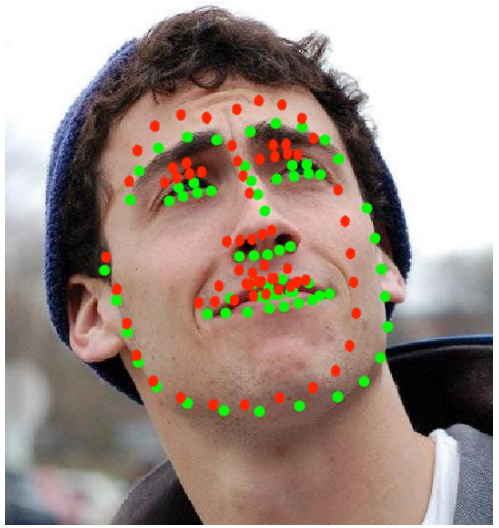
α^{id}

α^{exp}

3D Face Model

$$S = \bar{S} + A^{id}\alpha^{id} + A^{exp}\alpha^{exp}$$





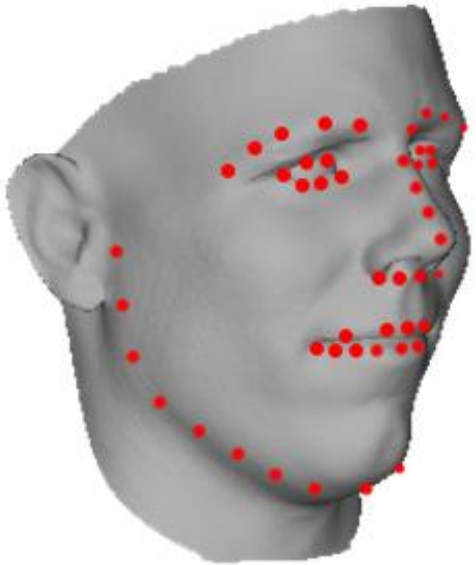
Pose

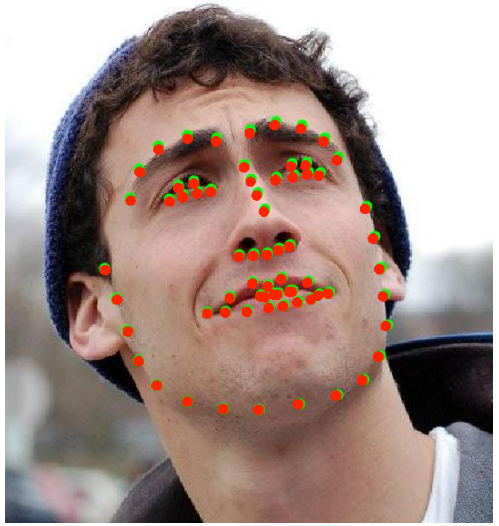
α^{id}

α^{exp}

3D Face Model

$$S = \bar{S} + A^{id}\alpha^{id} + A^{exp}\alpha^{exp}$$





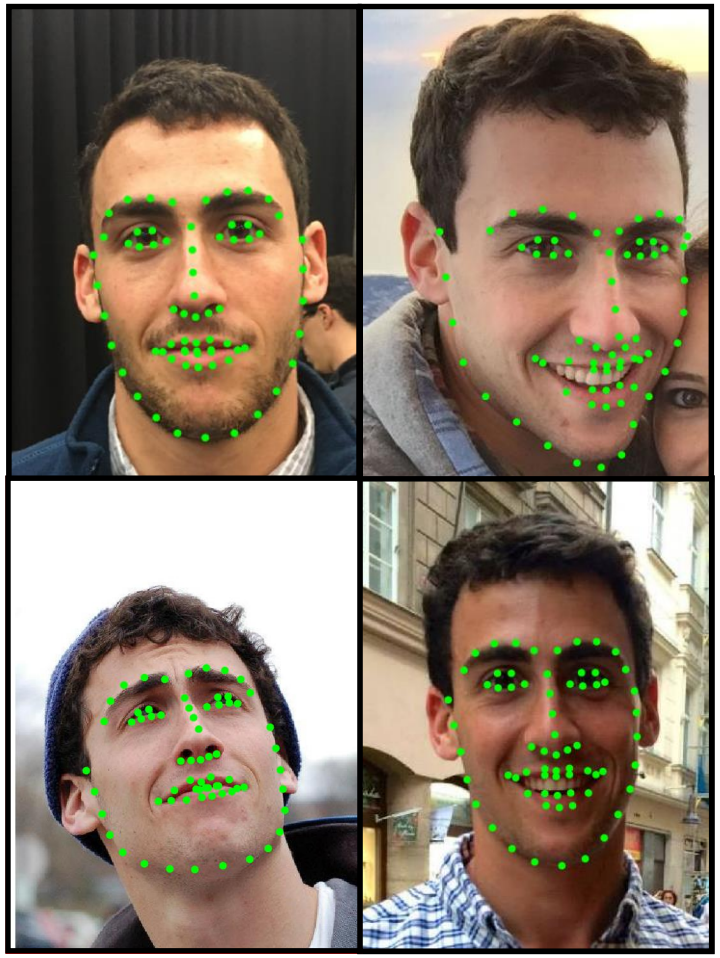
Pose

α^{id}

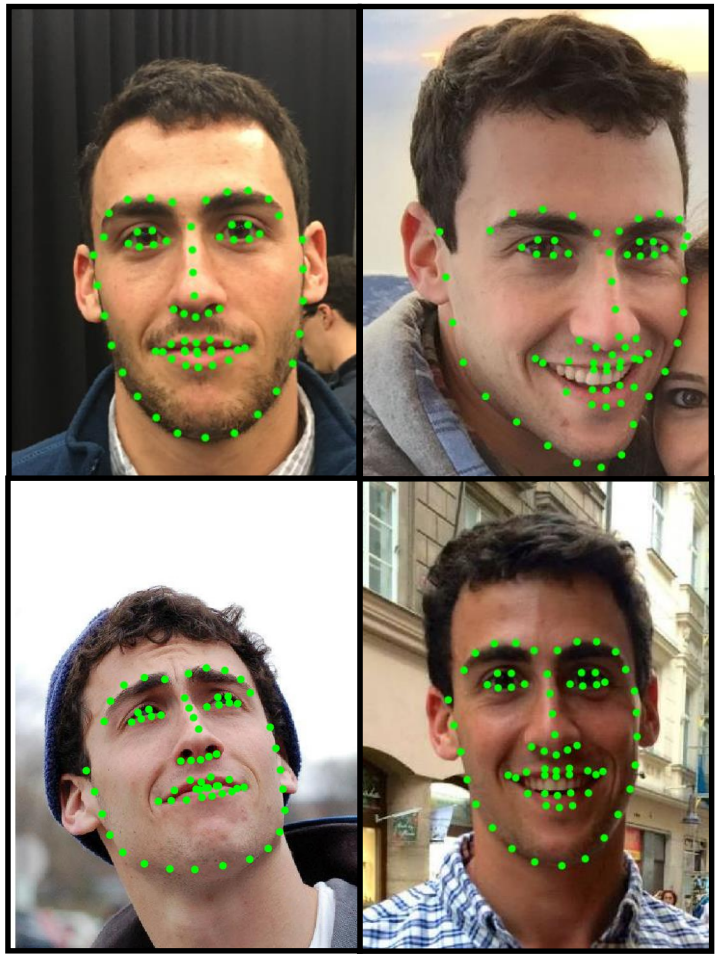
α^{exp}

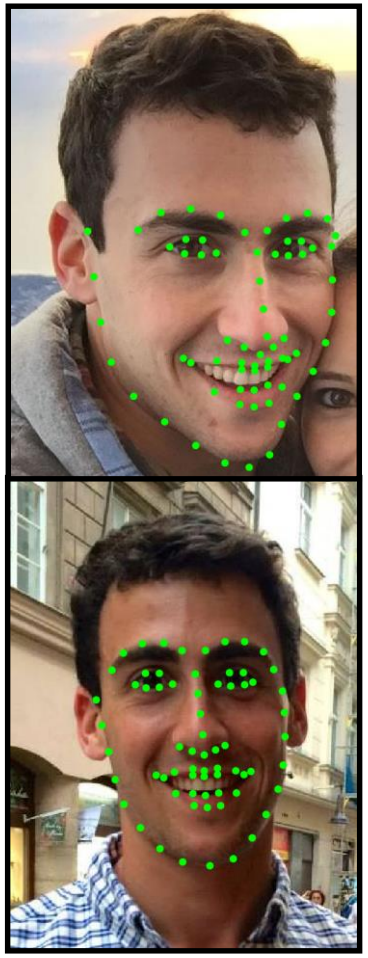
3D Face Model

3D Face Model

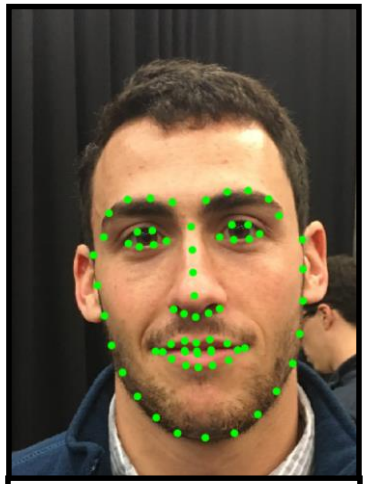


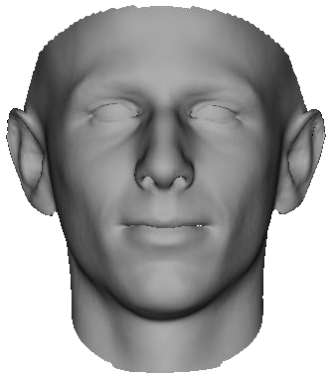
3D Face Model



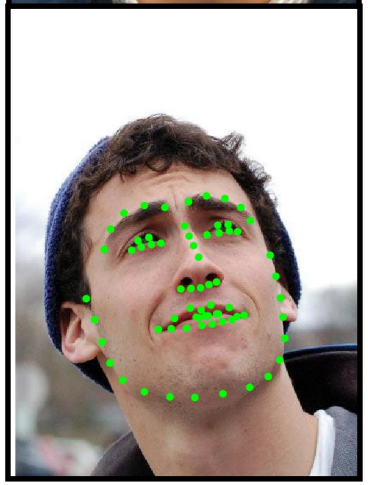


3D Face Model

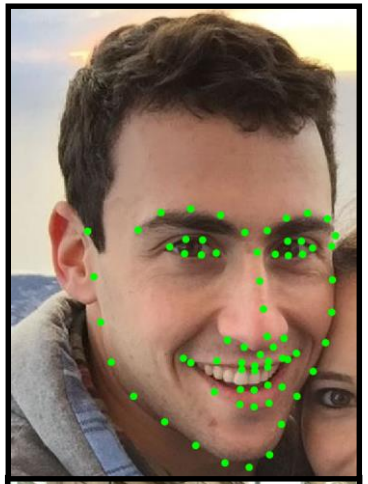




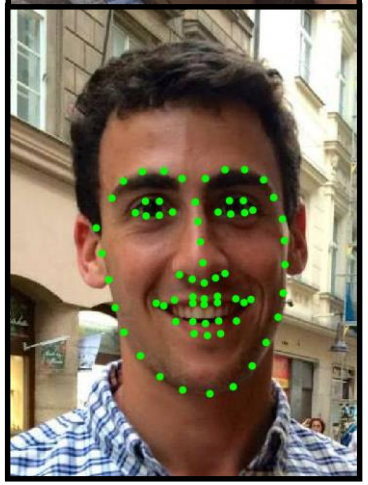
Pose α^{exp}

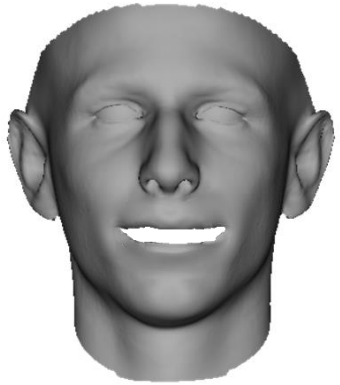


Pose α^{exp}



Pose α^{exp}

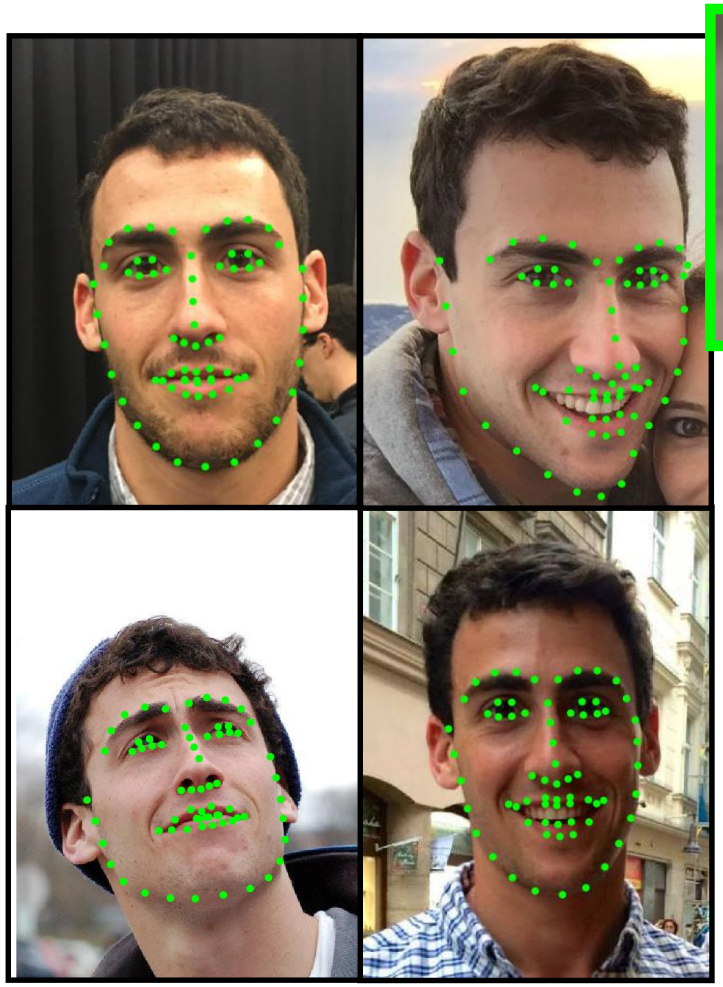


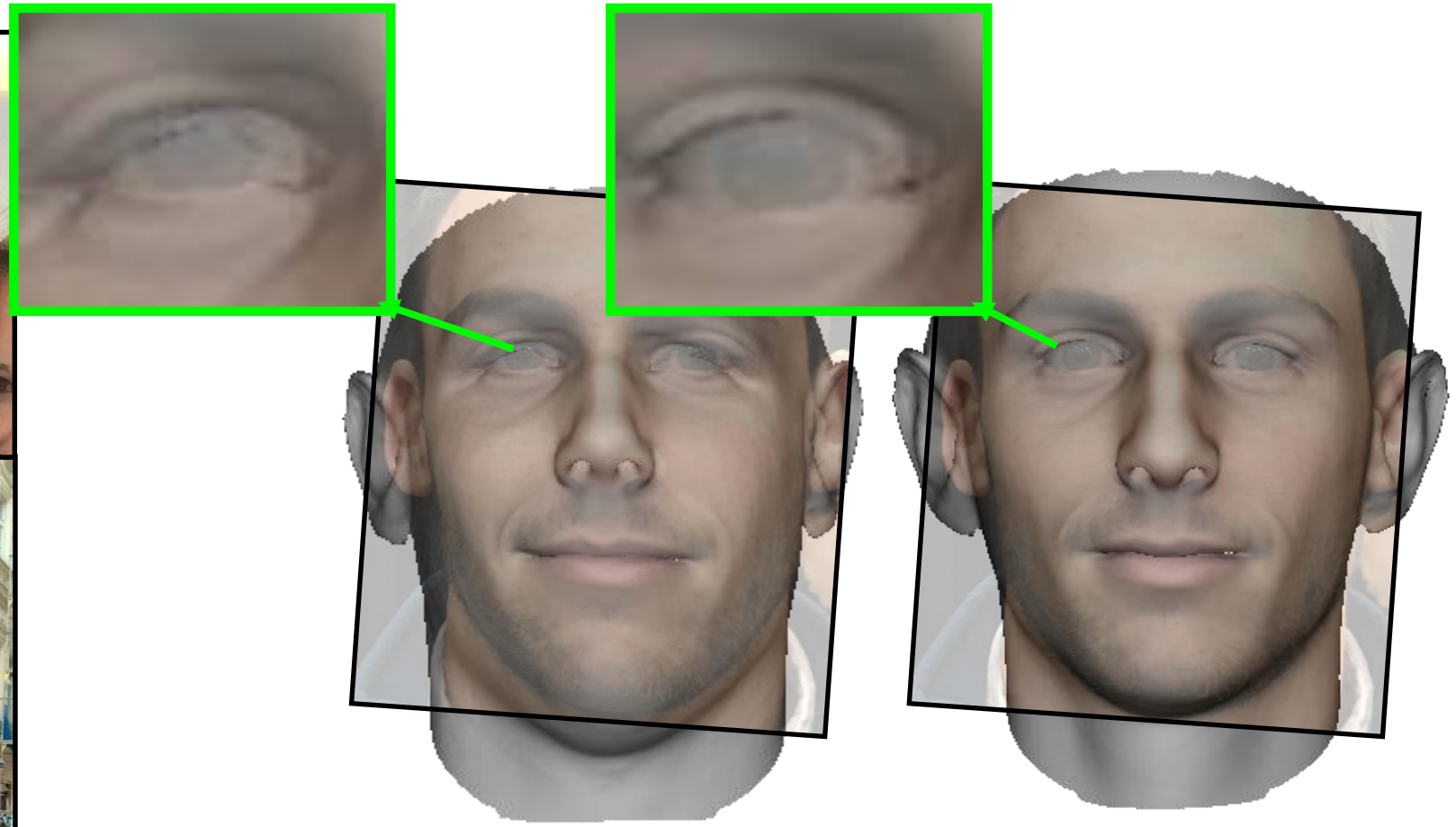


Pose α^{exp}

α^{id}

Multi-Image Modeling





Single image

Multiple images

Texturing

Direct Texturing

2D Poisson Editing

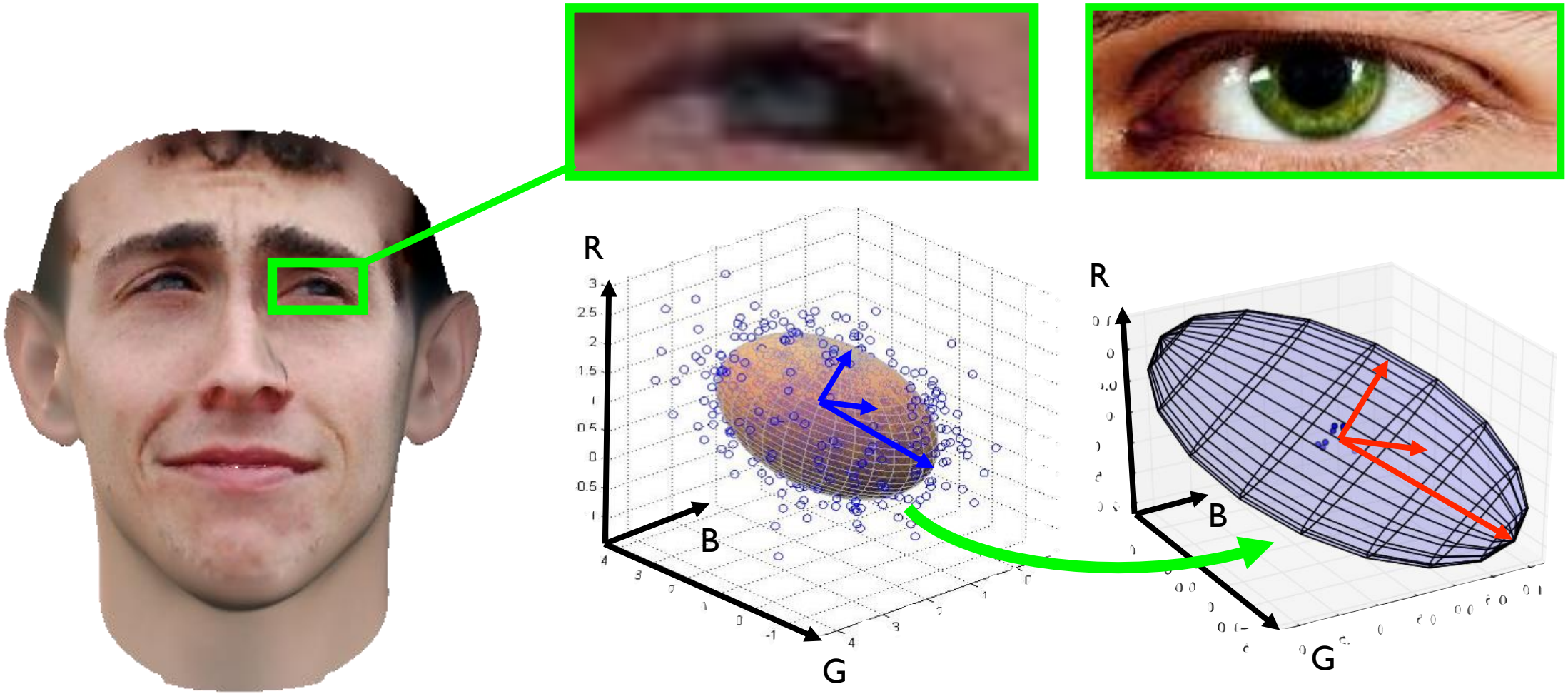
Texturing

Direct Texturing

2D Poisson Editing

3D Poisson Editing

Gaze Correction



Gaze Correction

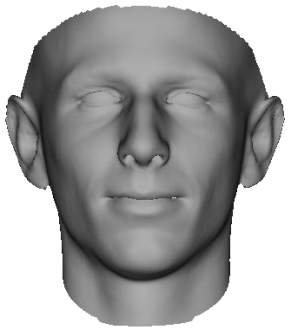
Virtual U: A New Attack

Input
Web Photos

1

Landmark
Extraction

2



3D Model
Reconstruction

3

Image-based
Texturing

4

Gaze
Correction

5

Expression Animation

6

Viewing with Virtual Reality System

Expression Animation

$$S = \bar{S} + A^{id}\alpha^{id} + A^{exp}\alpha^{exp}$$

Smiling | Laughing | Blinking | Raising Eyebrows

VR Display

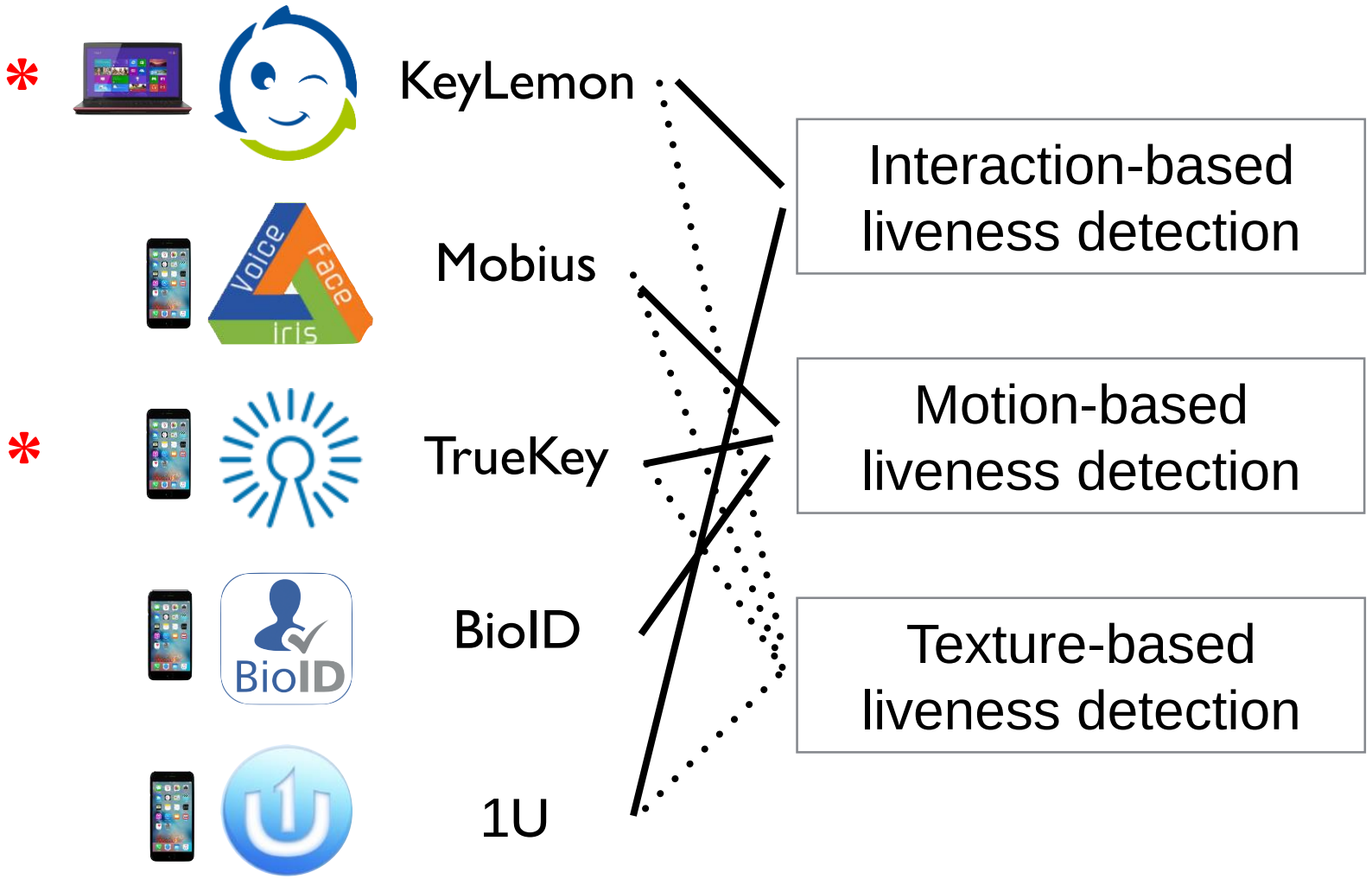
Printed Marker

VR System

Authentication Device

VR Display

Experiments

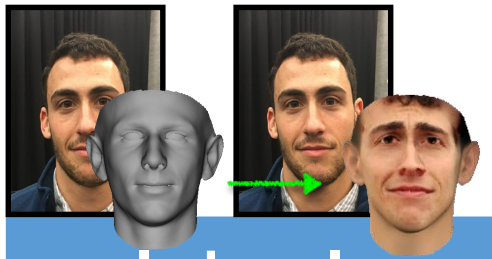


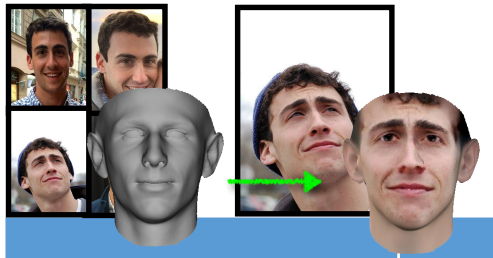
Experiments

- 20 participants
  - Aged 24 to 44
  - 14 males, 6 females
  - Various ethnicities

- Two tests
  - Indoor photo of the subject in the same environment as registration
  - Publicly accessible photos
    - Anywhere from 3 to 27 photos per person
    - Low-, medium-, and high-quality
    - Potentially strong changes in appearance over time

Experiments



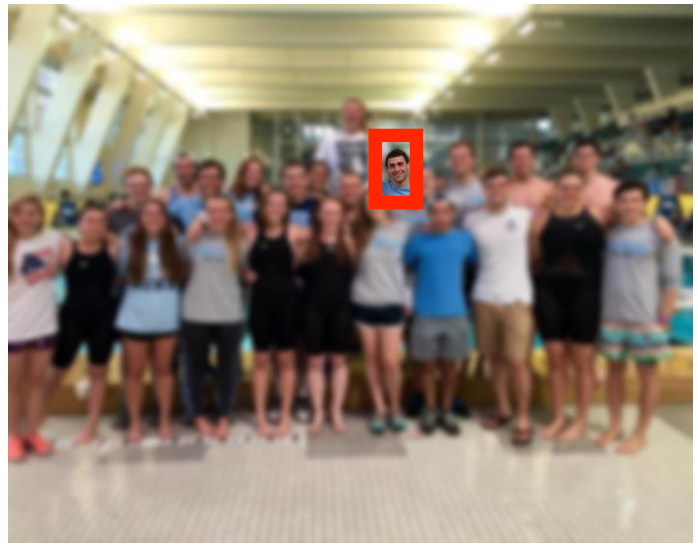


	Indoor Image (Single frontal image)	Online	Avg. # Tries
KeyLemon	100%	85%	1.6
Mobius	100%	80%	1.5
TrueKey	100%	70%	1.3
BioID	100%	55%	1.7
1U	100%	0%	--

Observations

- Medium- and high-resolution photos work best
  - Photos from professional photographers (weddings, etc.)

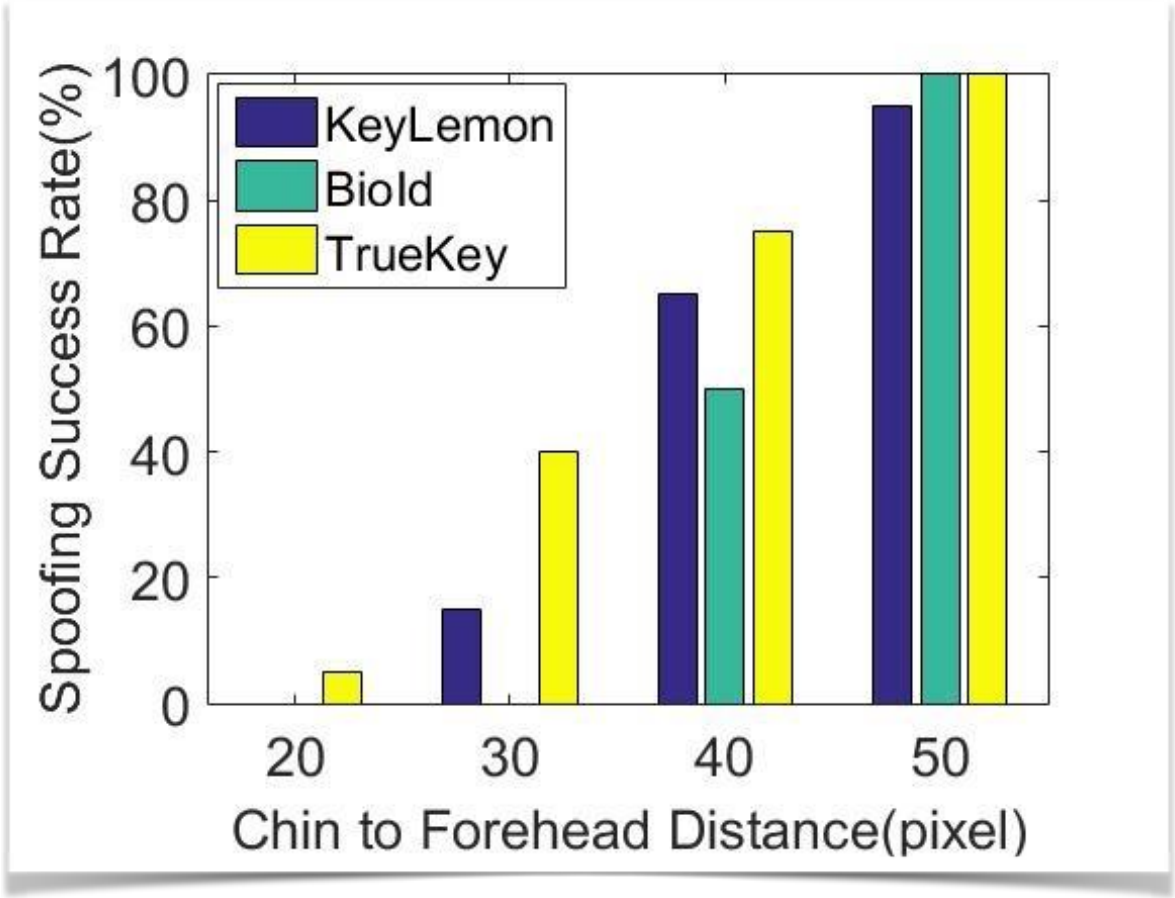
- Group photos provide consistent frontal views
  - Often lower resolution

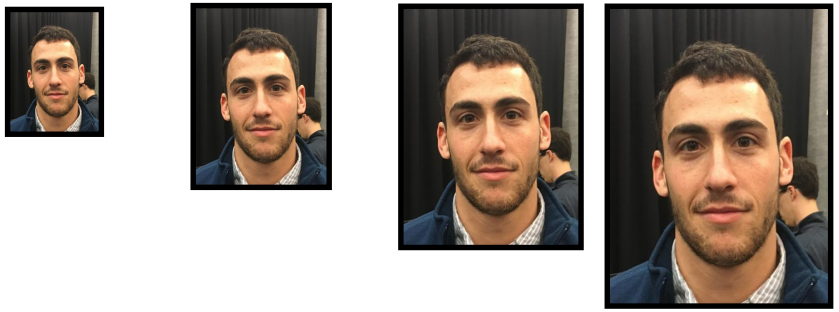


- Only a small number of photos required
  - One or two forward-facing photos
  - One or two higher-resolution photos

Experiments

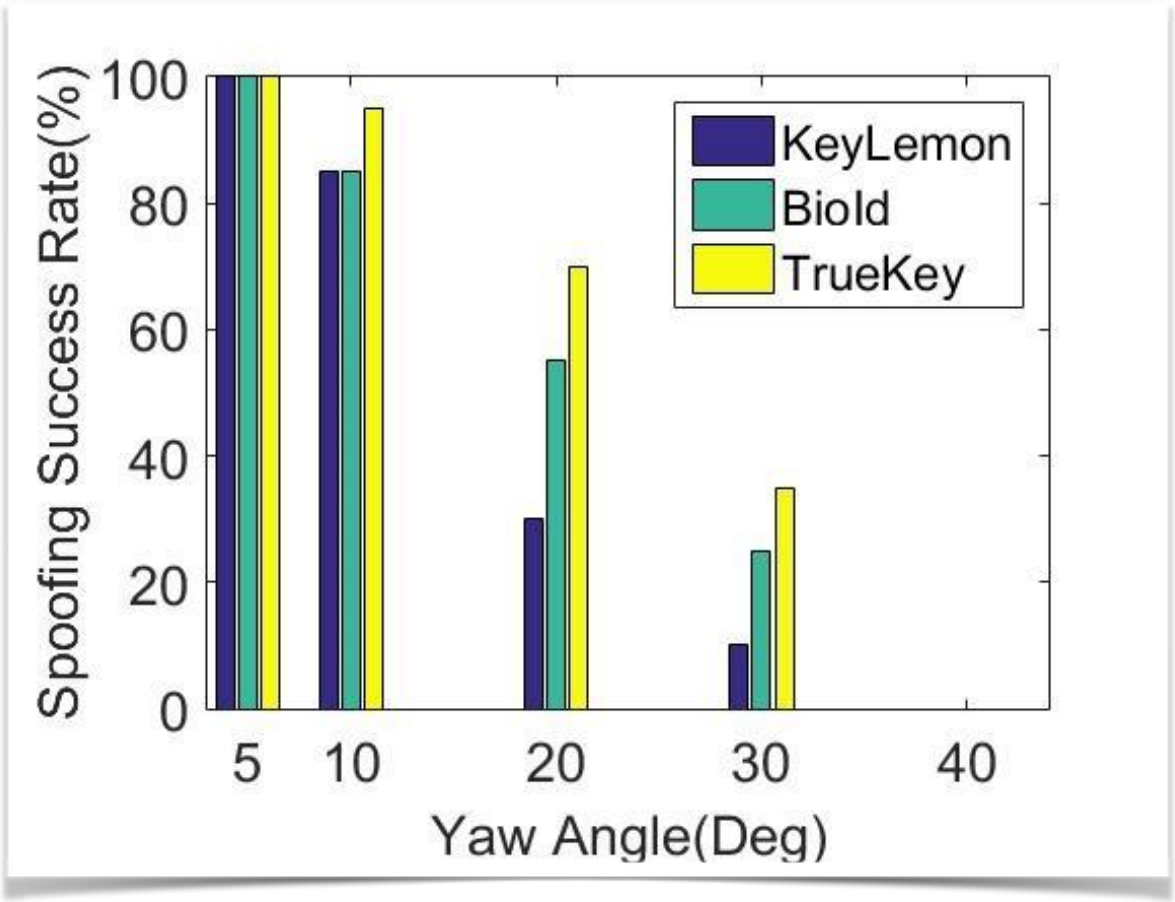
How does resolution affect reconstruction quality?





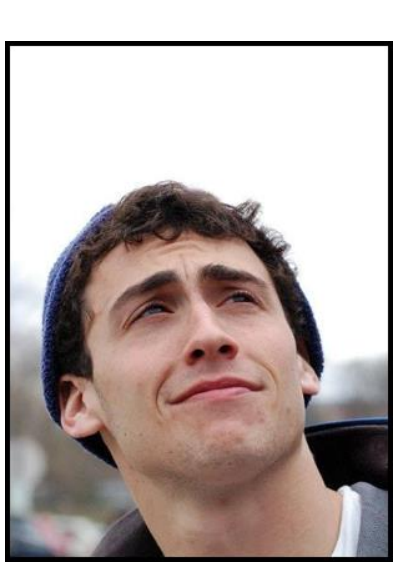
Experiments

How does rotation affect reconstruction quality?

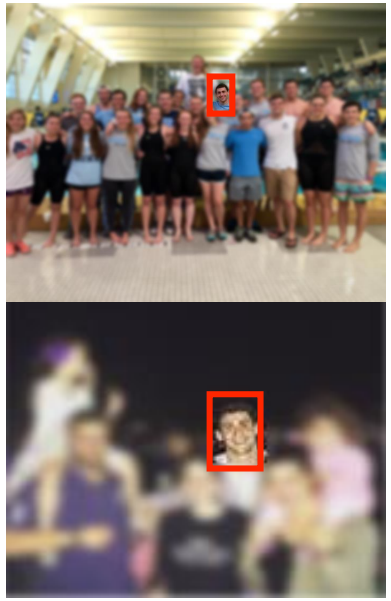


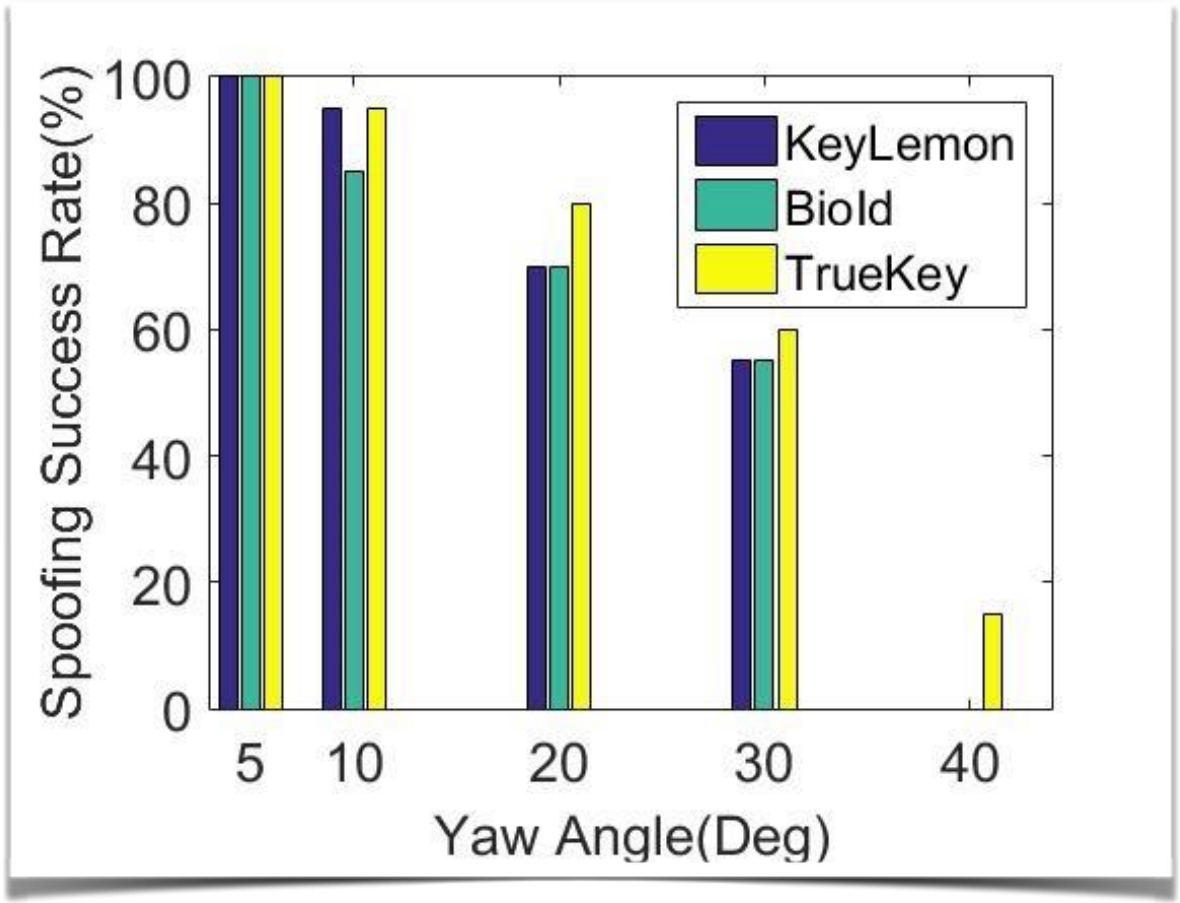
Experiments

Combining high-res rotation with low-res front-facing?



+





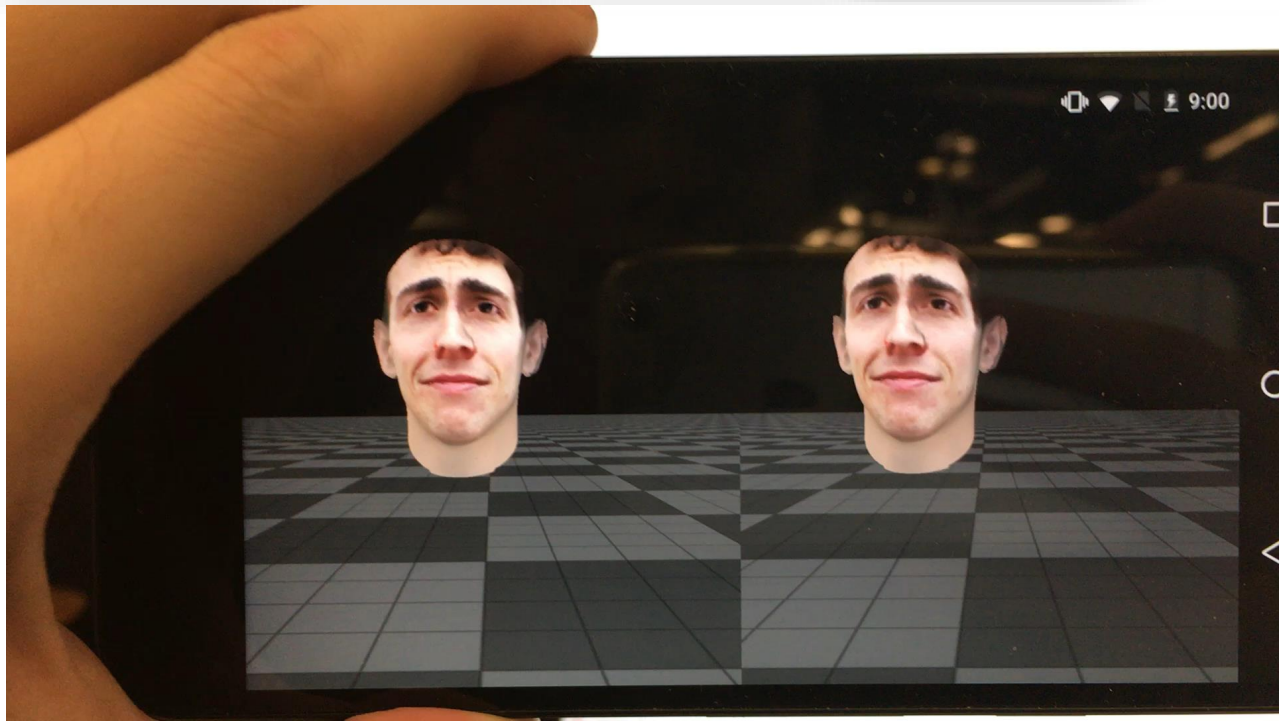
Experiments

- Virtual U is successful against liveness detection

Experiments

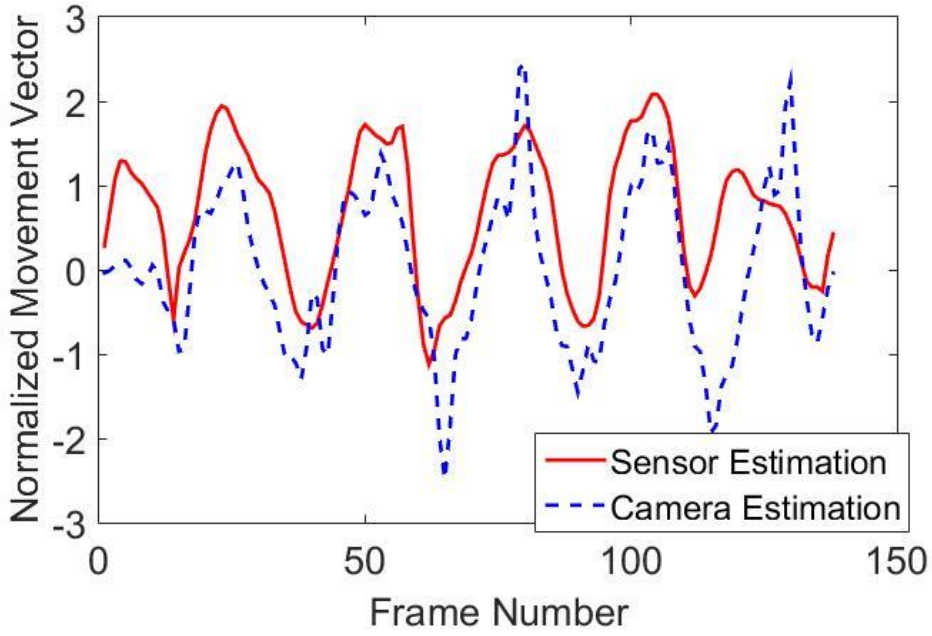
- Virtual U is successful against liveness detection

- Also successful against motion consistency

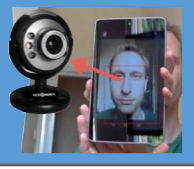


Experiments

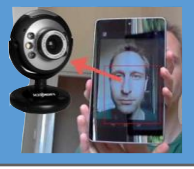
- "Seeing Your Face is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication" (Li et al., ACM CCS'15)
  - Device motion measured by inertial sensor data
  - Head pose estimated from input video
  - Train a classifier to identify real data (correlated signals) versus spoofed video data



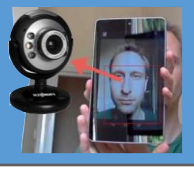
Experiments

Training Data (Pos. Data vs. Neg. Data)	Test Result (Accept Rate)		
	Real Face	Video Spoof 	VR Spoof 
Real vs. Video 	98.0%	1.3%	97.5%

Experiments

Training Data (Pos. Data vs. Neg. Data)	Test Result (Accept Rate)		
	Real Face	Video Spoof 	VR Spoof 
Real vs. Video 	98.0%	1.3%	97.5%
Real vs. Video  +VR 	70.0%	0.0%	50.0%

Experiments

Training Data (Pos. Data vs. Neg. Data)	Test Result (Accept Rate)		
	Real Face	Video Spoof 	VR Spoof 
Real vs. Video 	98.0%	1.3%	97.5%
Real vs. Video  +VR 	70.0%	0.0%	50.0%
Real vs. VR 	73.7%	-	50.0%

Mitigations

- Alternative/additional hardware
  - Infrared imaging (e.g. Windows Hello)
  - Random structured light projection

image source

Mitigations

- Alternative/additional hardware
  - Infrared imaging (e.g. Windows Hello)
  - Random structured light projection
- Improved defense against low-resolution synthetic textures

Original

Downsized to 50px

Conclusion

- We introduce a new VR-based attack on face authentication systems solely using publicly available photos of the victim
- This attack bypasses existing defenses of liveness detection and motion consistency
- At a minimum, face authentication software must improve against VR-based attacks with low-resolution textures
- The increasing ubiquity of VR will continue to challenge computer-vision-based authentication systems

Thank you!

Questions?