Viability of Optical Coherence Tomography for Iris Presentation Attack Detection

Renu Sharma, Arun Ross

{sharma90, rossarun}@cse.msu.edu

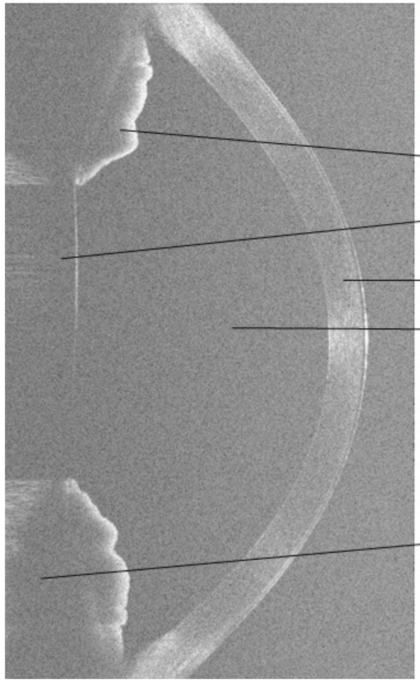
Michigan State University, USA

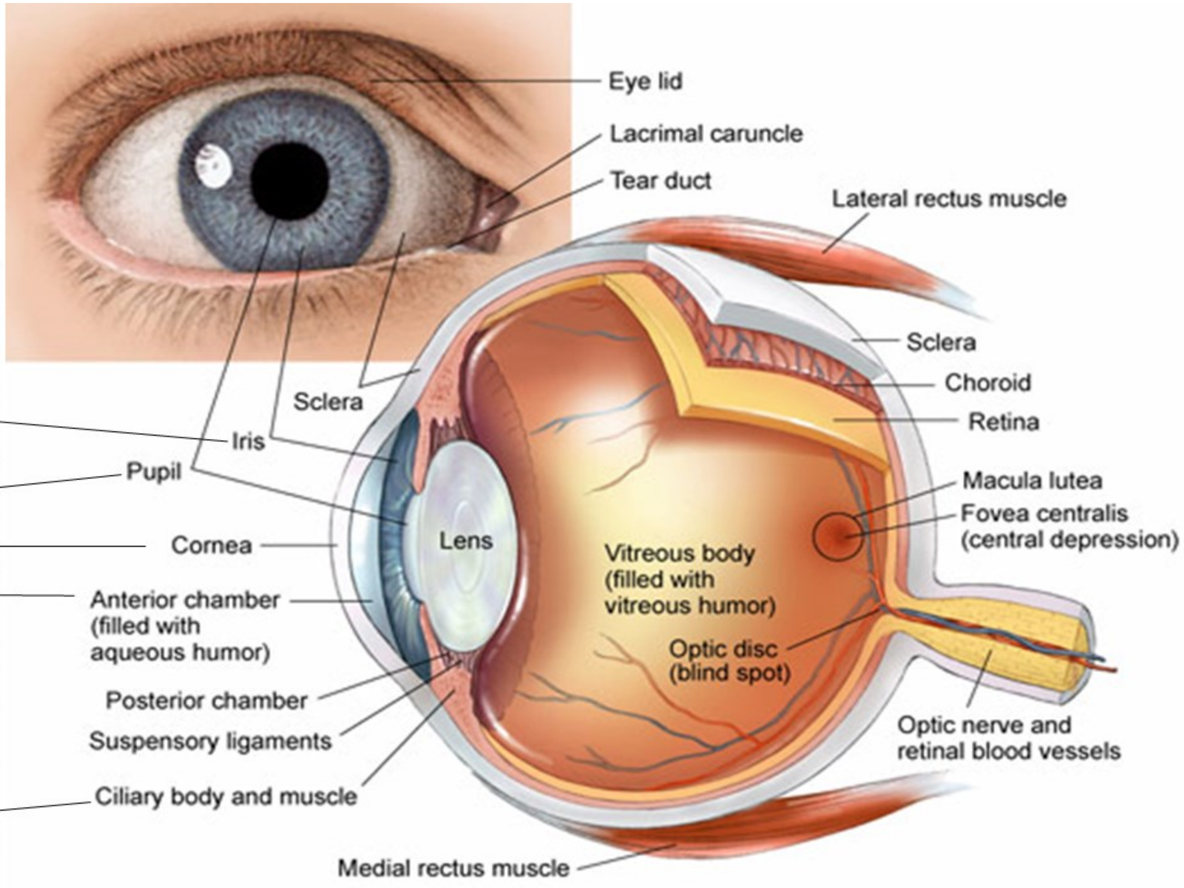
Research Sponsored by IARPA

Optical Coherence Tomography (OCT) Imaging

Optical Coherence Tomography (OCT) is non-invasive, micrometer-resolution imaging that captures 2-D cross-sectional or 3-D volumetric images of an object in the NIR spectrum

OCT Image





Right Eye (viewed from above)

https://eye-courses.com/product/basic-anatomy-2/

Iris Presentation Attack

A presentation attack (PA) occurs when an adversarial user presents a fake or altered biometric sample to the sensor in order to spoof another user's identity, obfuscate their own identity, or create a virtual identity.

Print

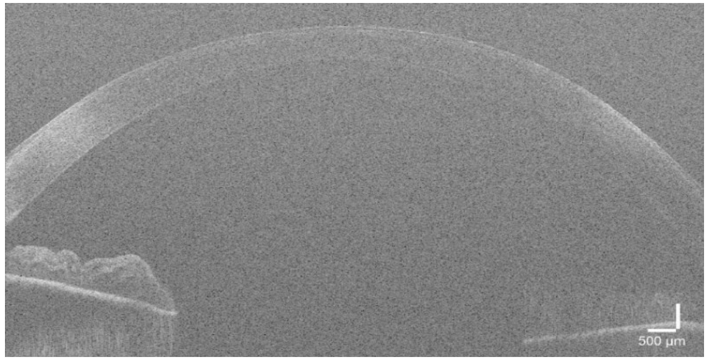
Plastic and Glass

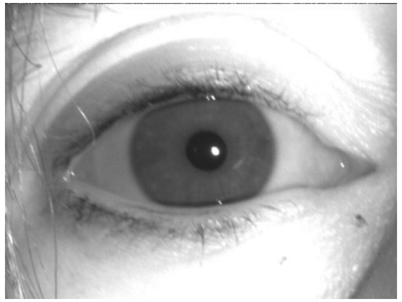
Cosmetic Lens

Motivation

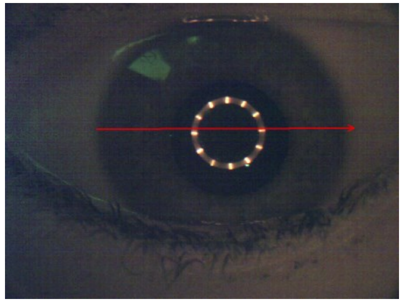
- Bonafide OCT images show a cross-sectional view of cornea and iris
- Fake eye OCT images show a thin line corresponding to the fake eye outer structure
- The cosmetic contact lens also blocks light, which creates gaps in the cornea structure

Bonafide



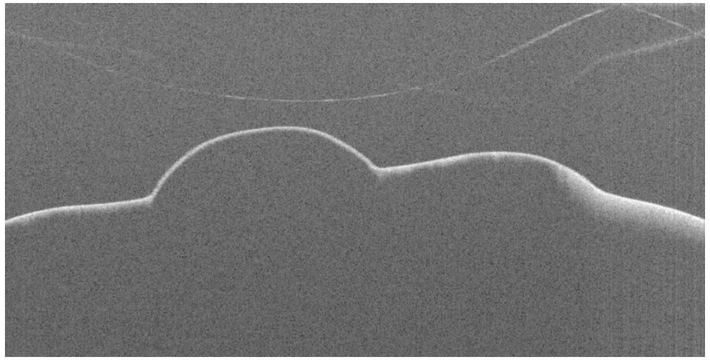


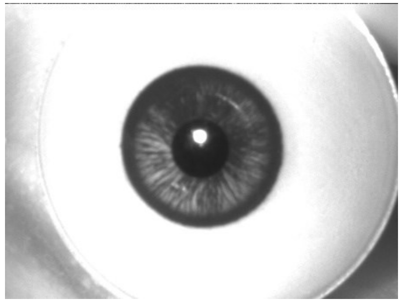
NIR



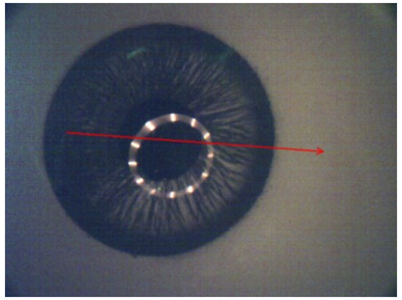
RGB

Fake Eye



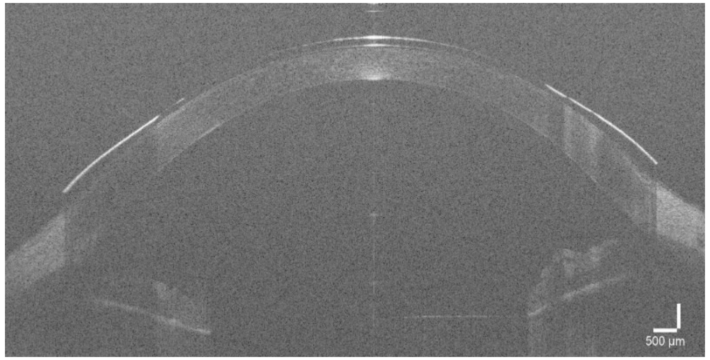


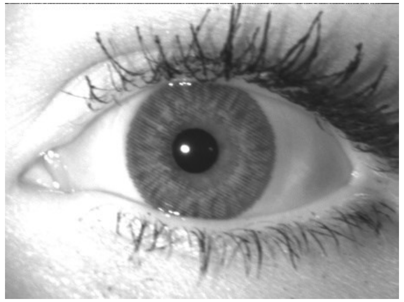
NIR



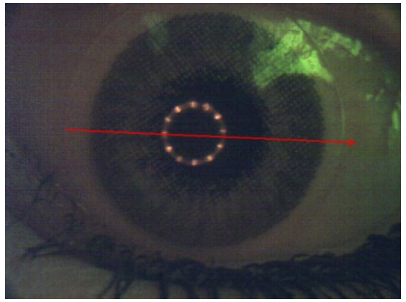
RGB

Cosmetic Contact Lens





NIR



RGB

Main Contributions

- Propose an iris PA detection technique based on OCT imaging modality
- Compare the performance of OCT, Near-Infrared (NIR), and Visible (RGB) imaging modalities using VGG19, ResNet50, and DenseNet121 deep architectures
- Perform the experiments on a proprietary dataset of 370 subjects collected from each modality
- Explain the results using CNN visualizations: Grad-CAM heatmaps and t-SNE plots

Implementation Details

- Utilize pre-trained VGG19[1], ResNet50 [2] and DenseNet121[3] models trained on ImageNet dataset [4] which further fine-tuned with OCT, NIR and RGB iris PA data
- Images are resized to 224 x 224 and normalized using z-score before input
  - This helps in regulating the weight parameters
- Learning rate = 0.005, batch size= 20, and no. of epochs = 50

1. K. Simonyan and A. Zisserman. Very deep convolutional networks for large-scale image recognition. ICLR, 2015.
2. K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. CVPR, 2016.
3. G. Huang, Z. Liu, L. v. d. Maaten, and K. Q. Weinberger. Densely connected convolutional networks. CVPR, 2017.
4. J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, ImageNet: A Large-Scale Hierarchical Image Database. CVPR, 2009.

Dataset and Experimental Setup

- The dataset collected under the Odin program of IARPA from 370 subjects contains 844 bonafide, 61 fake eyes, and 120 cosmetic contact (CC) images
- OCT, NIR and VIS images are captured using Telesto series OCT sensor, RGB camera, and iCAM7000 NIR sensor, respectively
- Experiments are performed under intra and cross-attack scenarios

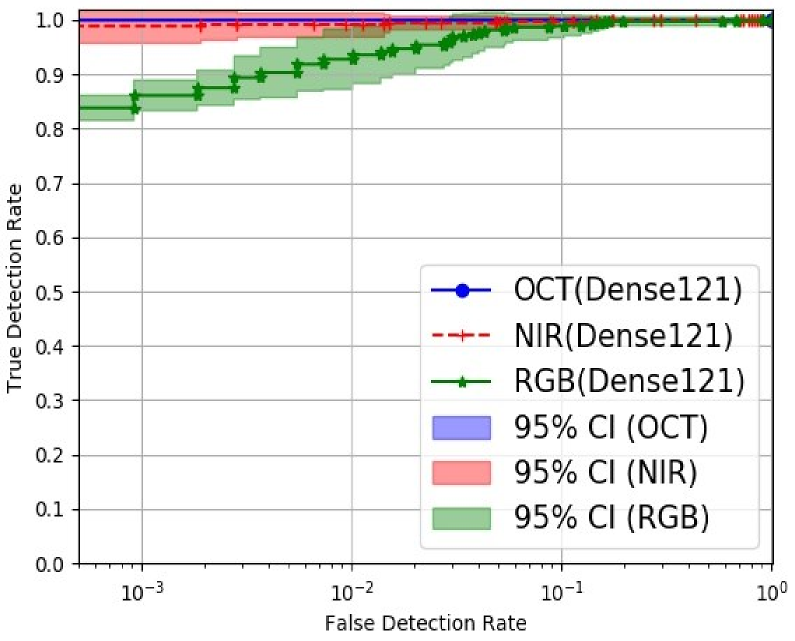
Experiments	Train Set		Validation Set		Test Set	
	Bonafide	**PAs**	**Bonafide**	**PAs**	**Bonafide**	**PAs**
Intra-EXP (Fold 01-05)	404	100	101	25	218	54
Cross-EXP 1 (CC Lenses are unknown)	435	41 (Fake Eyes)	145	18 (Fake Eyes)	146	120 (CC)
Cross-EXP 2 (Fake eyes are unknown)	435	84 (CC)	145	36 (CC)	146	59 (Fake Eyes)

Experimental Results

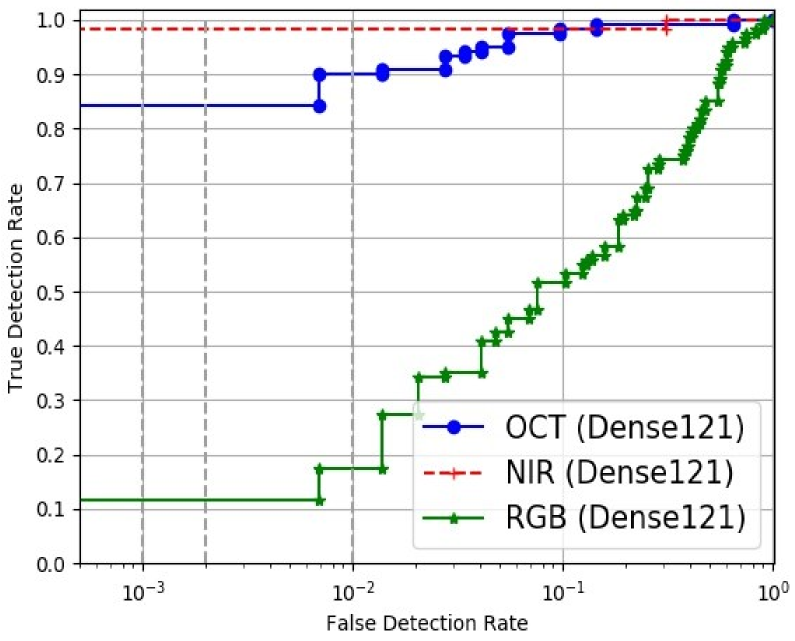
	True Detection Rate (%) at 0.2% False Detection Rate								
Experiments	VGG19			ResNet50			DenseNet121		
	OCT	NIR	RGB	OCT	NIR	RGB	OCT	NIR	RGB
Intra-EXP	**100 ± 0.00**	97.99 ± 2.66	82.58 ± 6.88	**100 ± 0.00**	97.33 ± 3.88	89.62 ± 3.62	**100 ± 0.00**	97.66 ± 3.26	86.66 ± 3.59
Cross-EXP 1 (CC are unknown)	21.66	**97.58**	26.66	92.50	**98.38**	15.00	84.16	**98.38**	11.66
Cross-EXP 2 (Fake eyes are unknown)	86.44	**98.38**	93.22	94.91	**96.77**	81.35	94.91	**96.77**	91.52

OCT images better discriminate between bonafide and PAs under known PAs scenario, whereas NIR images perform better across unknown PAs scenario

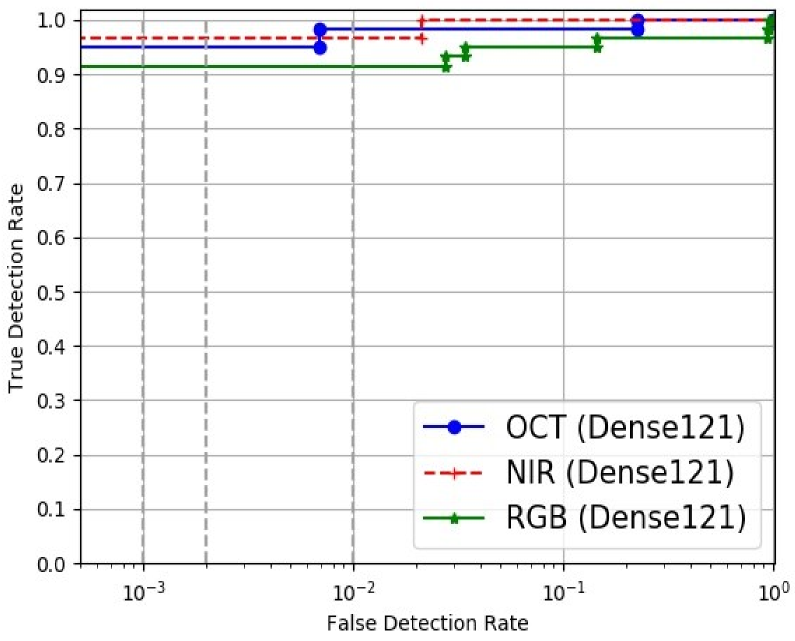
Experimental Results: ROC Curves [DenseNet121]



Intra-EXP



Cross-EXP 1
(CC are unknown)

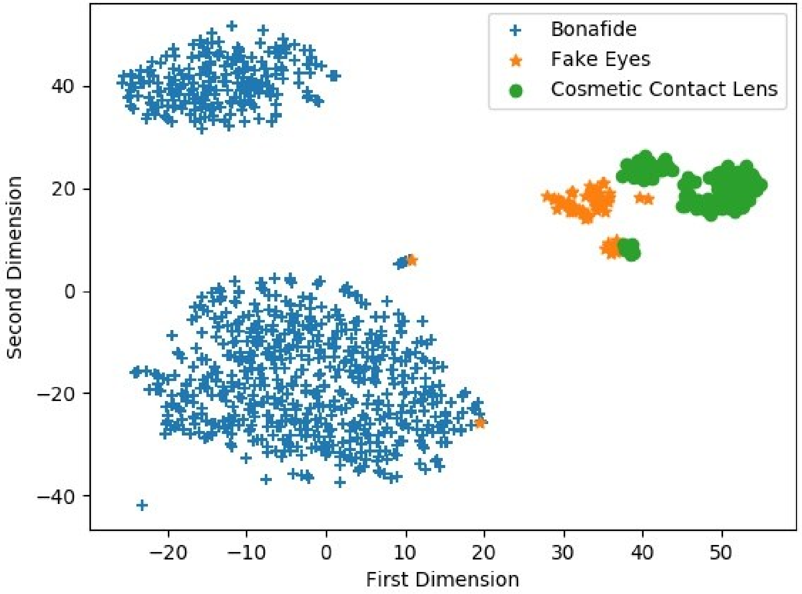


Cross-EXP 2
(Fake eyes are unknown)

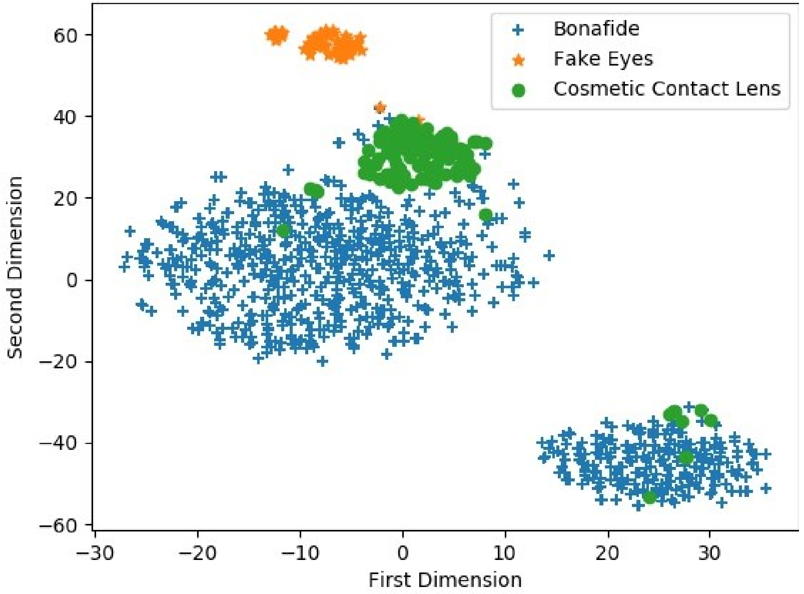
OCT imaging performs better under intra-attack scenario and
NIR imaging performs better under cross-attack scenario

Explainability: t-SNE Plots

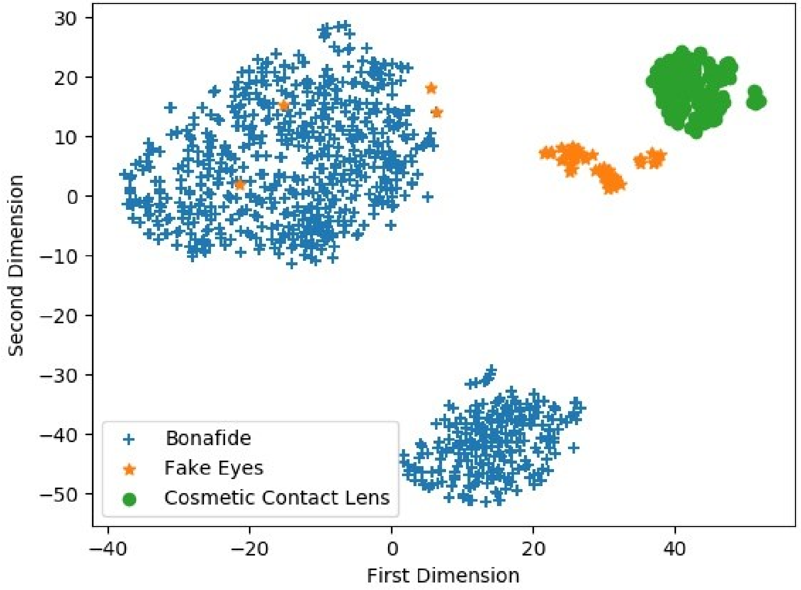
t-SNE helps in visualizing the high-dimensional features in a scatter plot



Intra-EXP



Cross-EXP 1
(CC are unknown)



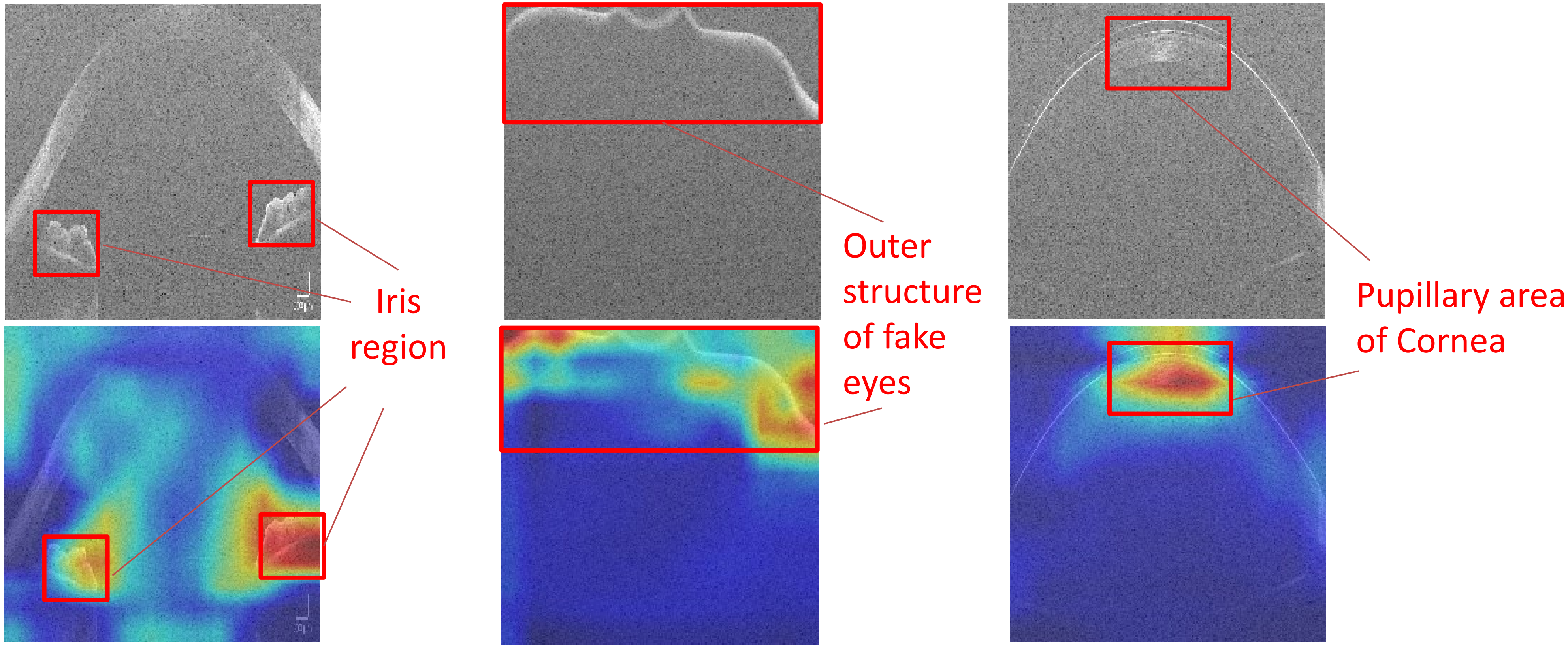
Cross-EXP 2
(Fake eyes are unknown)

Distribution of bonafide and PAs are better separated in Intra-EXP and Cross-EXP 2

1. van der Maaten, L.J.P. and Hinton, G.E.., **Visualizing High-Dimensional Data Using t-SNE**, 2008.

Explainability: Grad-CAM Heatmaps

Heatmaps emphasize the salient regions utilize by the network to detect PAs



Bonafide | Fake Eye | Cosmetic Contact

Red-colored regions represent highly focused regions, whereas the blue region represents low priority regions

Distinctive region of focus in each category helps in distinguishing bonafides and PAs

1. R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh and D. Batra, **Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization**, ICCV,2017.

Conclusion and Future Work

- Proposed a viable solution for iris PA detection based on OCT imaging
- It gives near-perfect performance on a small dataset set under intra-attack scenario, whereas NIR imaging generalizes better under cross-attack scenario
- The performance is explained using t-SNE and Grad-CAM plots
- Future work: to collect more OCT iris data along with other types of PAs using different types of OCT hardware
- Hardware cost is one of the current limitations

Acknowledgment

- This project is funded by Intelligence Advanced Research Projects Activity (IARPA)
- This research is based upon work supported in part by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via IARPA R&D Contract No. 2017 - 17020200004. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

Any
questions?

Email: sharma90@cse.msu.edu