# Convolutional Neural Networks: Epic Fails

Laura E. Boucheron

College of Engineering | Klipsch School of Electrical & Computer Engineering


BE BOLD. Shape the Future.

**Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 427-436).**

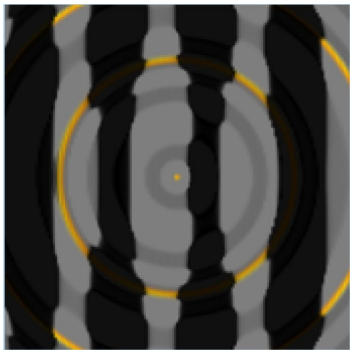
Penguin (99.99%)

Electric Guitar (98.90%)

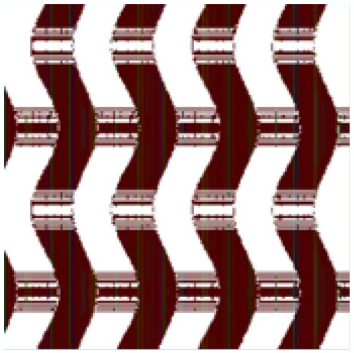


All figures on this slide taken from the reference at the top

**Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 427-436).**



Penguin (99.99%)



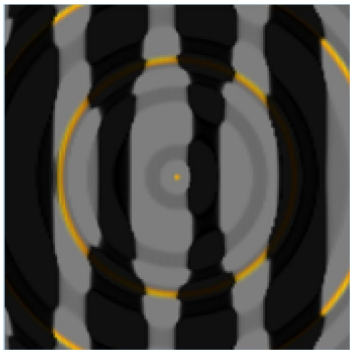
Electric Guitar (98.90%)



All figures on this slide taken from the reference at the top

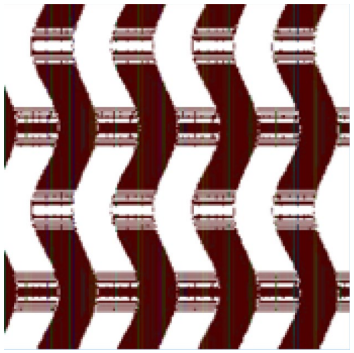
**Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 427-436).**

Penguin (99.99%)



Penguin (99.99%)

Electric Guitar (98.90%)



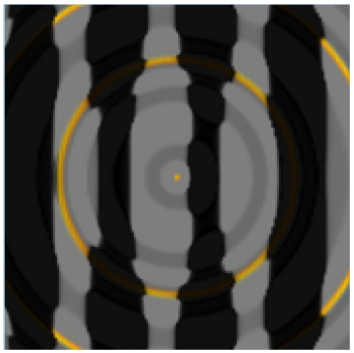
Electric Guitar (99.99%)



All figures on this slide taken from the reference at the top

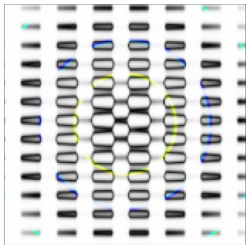
**Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 427-436).**

Penguin (99.99%)

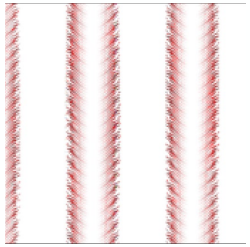


Penguin (99.99%)

Other >99.5% confidence predictions:

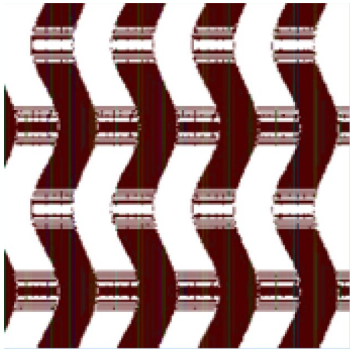


Remote control



Baseball

Electric Guitar (98.90%)



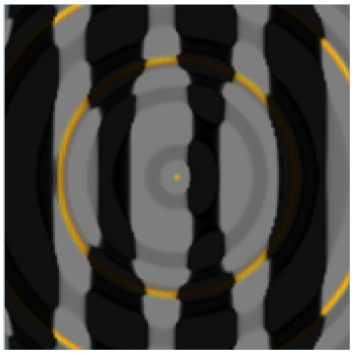
Electric Guitar (99.99%)



All figures on this slide taken from the reference at the top

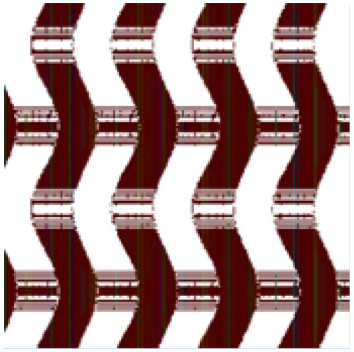
**Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 427-436).**

Penguin (99.99%)



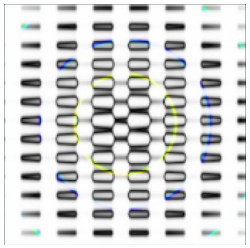
Penguin (99.99%)

Electric Guitar (98.90%)

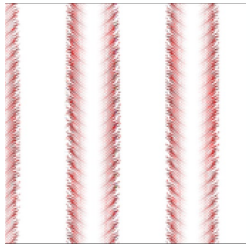


Electric Guitar (99.99%)

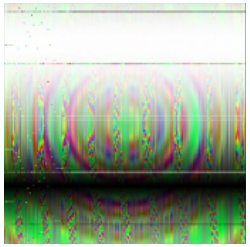
Other >99.5% confidence predictions:



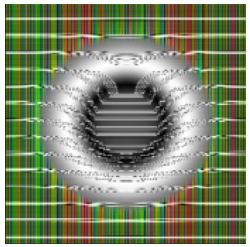
Remote control



Baseball



Freight car



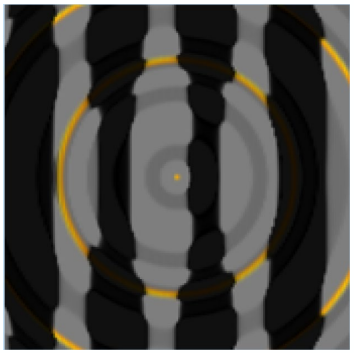
African grey



All figures on this slide taken from the reference at the top

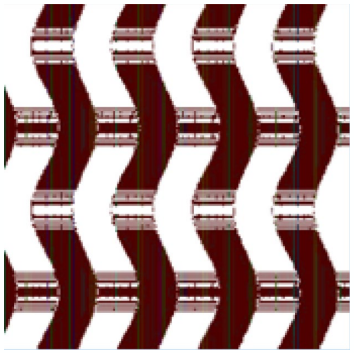
**Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 427-436).**

Penguin (99.99%)



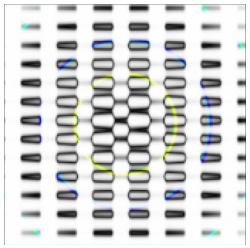
Penguin (99.99%)

Electric Guitar (98.90%)

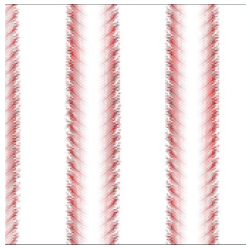


Electric Guitar (99.99%)

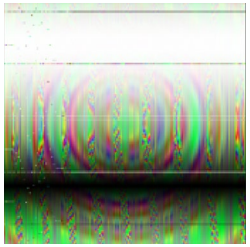
Other >99.5% confidence predictions:



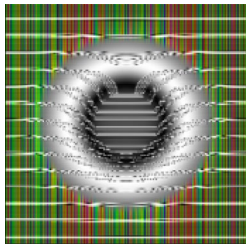
Remote control



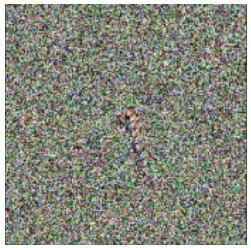
Baseball



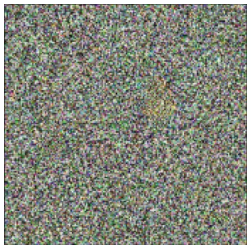
Freight car



African grey



Cheetah



Jackfruit



All figures on this slide taken from the reference at the top

**Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.**


School Bus



All figures on this slide taken from the reference at the top

**Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.**


School Bus




All figures on this slide taken from the reference at the top

**Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.**


School Bus

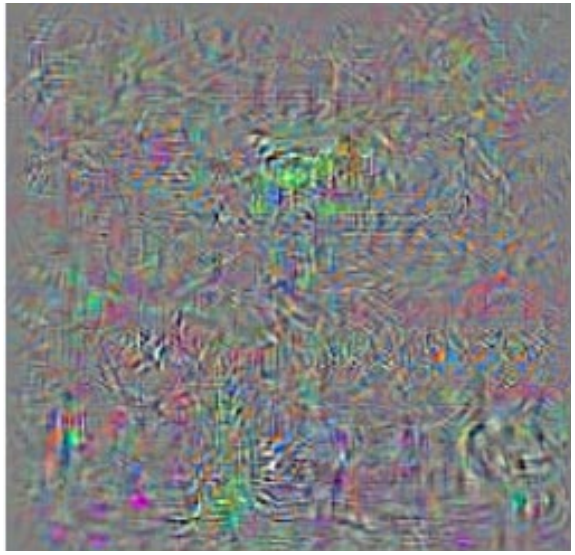

Ostrich



All figures on this slide taken from the reference at the top

**Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.**


School Bus



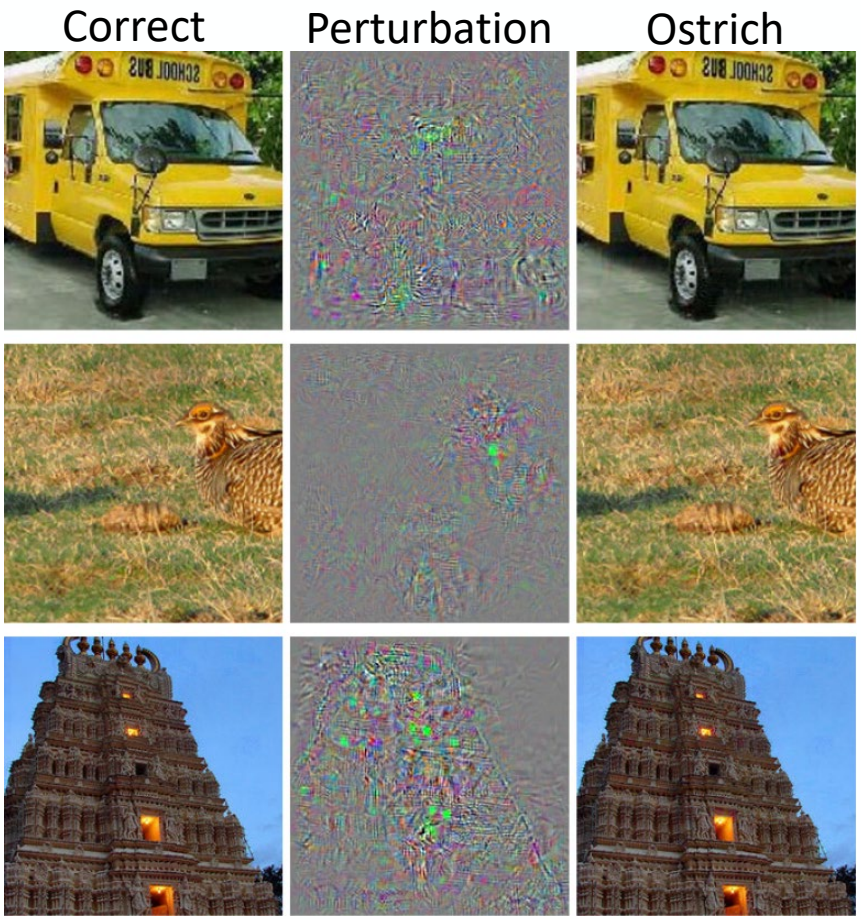
Perturbation

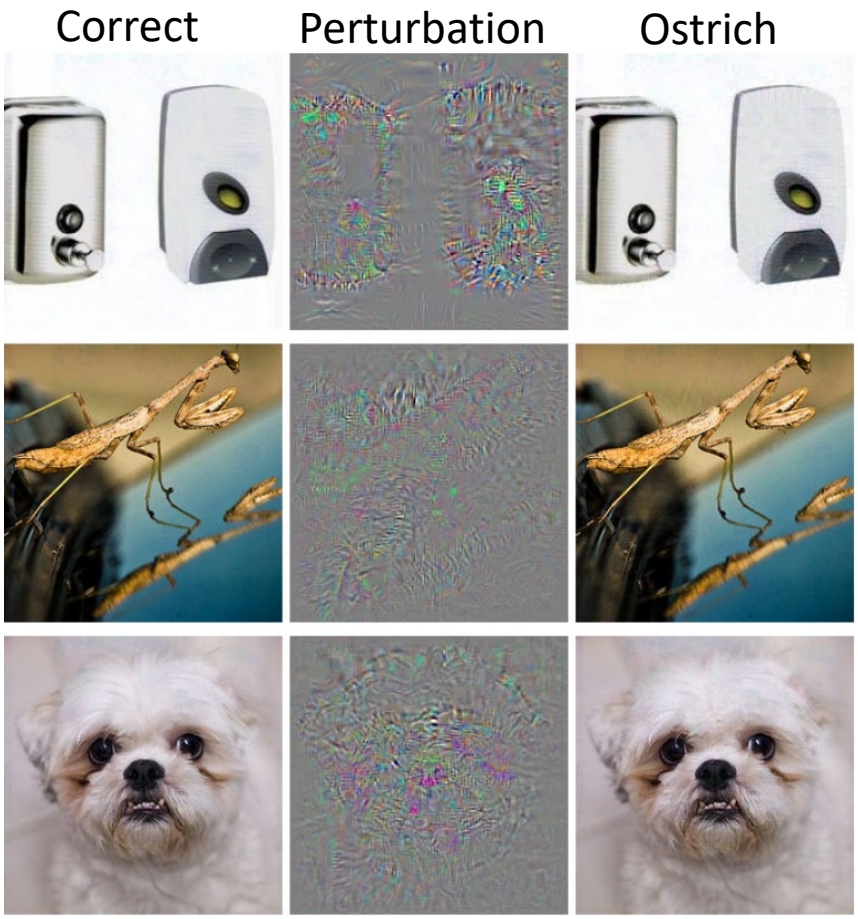

Ostrich



All figures on this slide taken from the reference at the top

**Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*.**



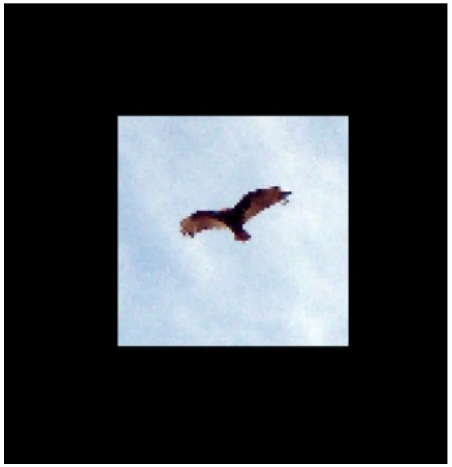






All figures on this slide taken from the reference at the top

**Engstrom, L., Tran, B., Tsipras, D., Schmidt, L., & Madry, A. (2017). A rotation and a translation suffice: Fooling cnns with simple transformations.** ***arXiv preprint arXiv:1712.02779*****.**


revolver



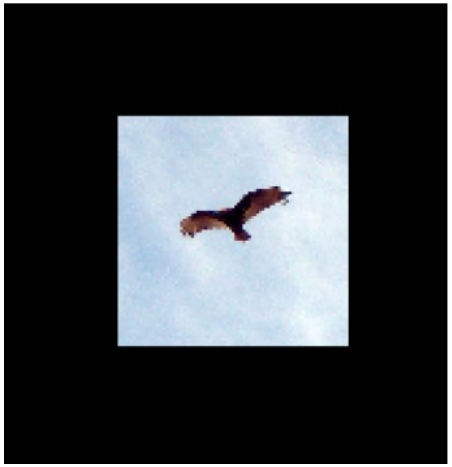
vulture



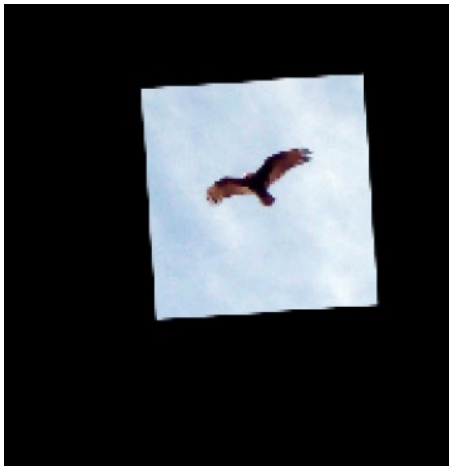
All figures on this slide taken from the reference at the top

**Engstrom, L., Tran, B., Tsipras, D., Schmidt, L., & Madry, A. (2017). A rotation and a translation suffice: Fooling cnns with simple transformations.** ***arXiv preprint arXiv:1712.02779*****.**


revolver



vulture

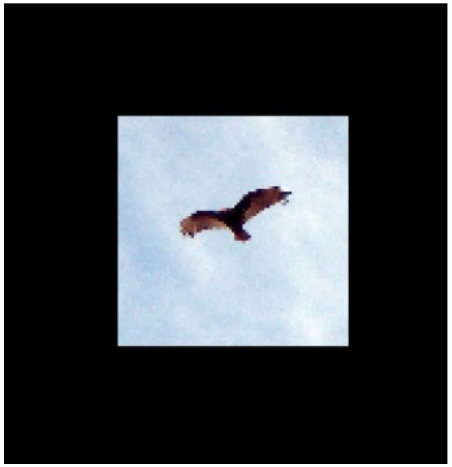





All figures on this slide taken from the reference at the top

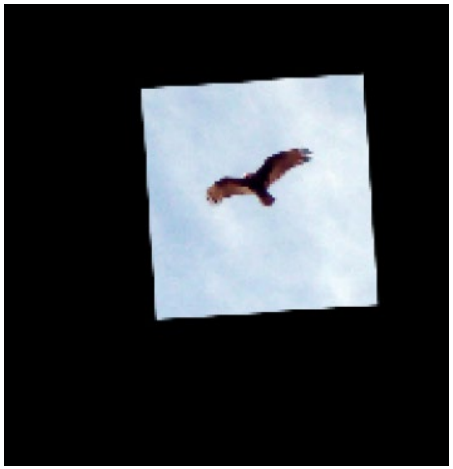
**Engstrom, L., Tran, B., Tsipras, D., Schmidt, L., & Madry, A. (2017). A rotation and a translation suffice: Fooling cnns with simple transformations.** ***arXiv preprint arXiv:1712.02779*****.**


revolver



vulture


mousetrap

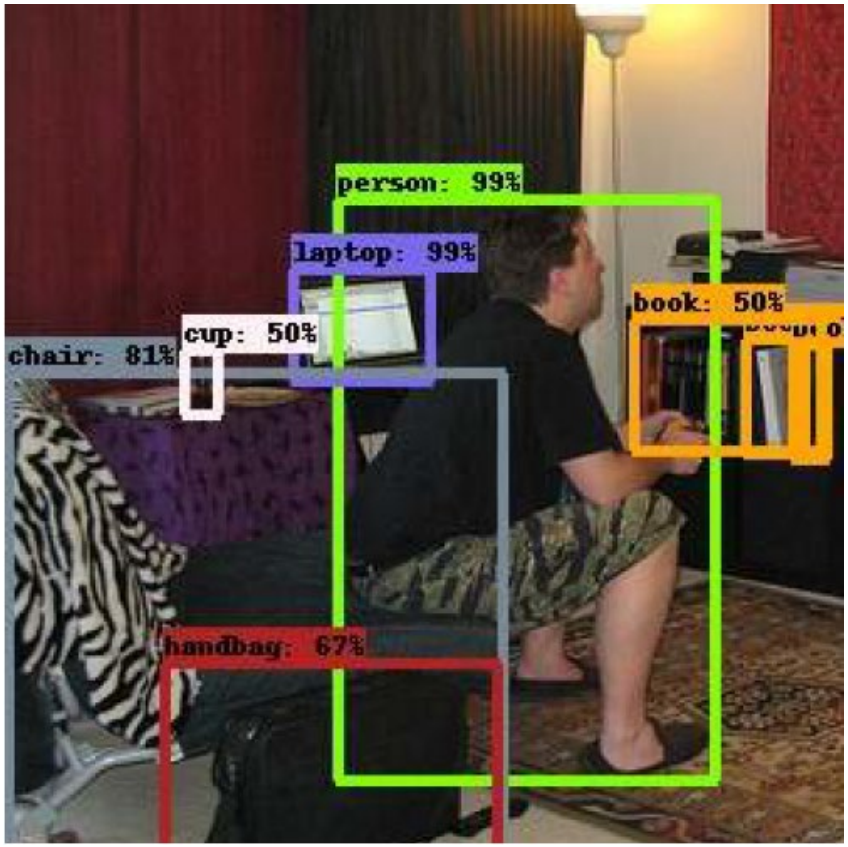


orangutan



All figures on this slide taken from the reference at the top

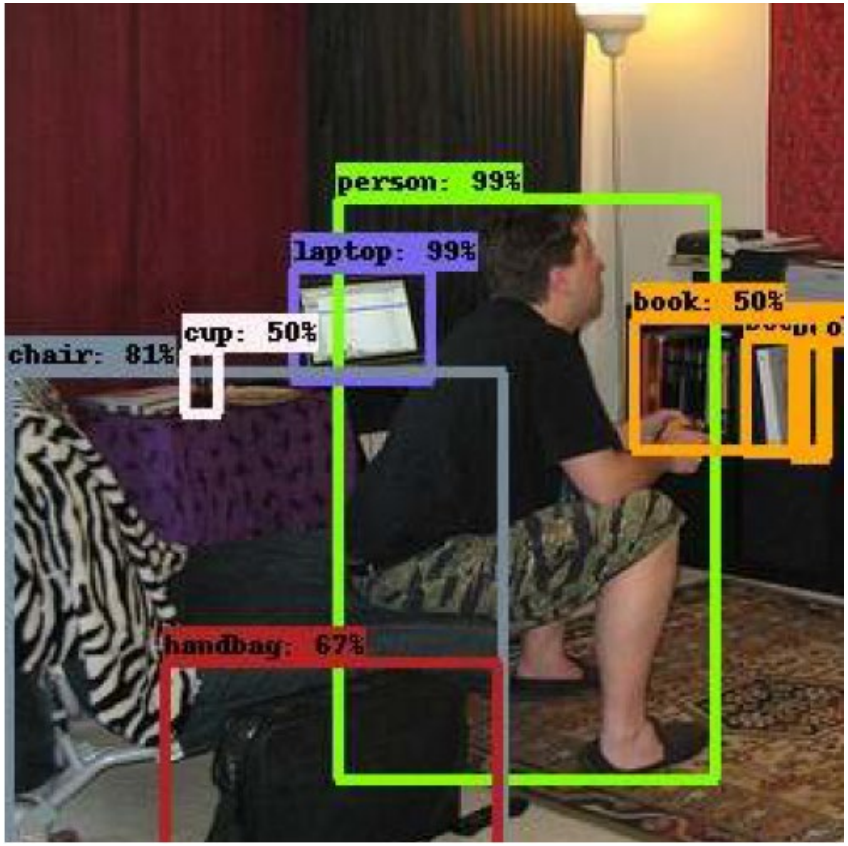
**Rosenfeld, A., Zemel, R., & Tsotsos, J. K. (2018). The elephant in the room.** ***arXiv preprint arXiv:1808.03305*****.**

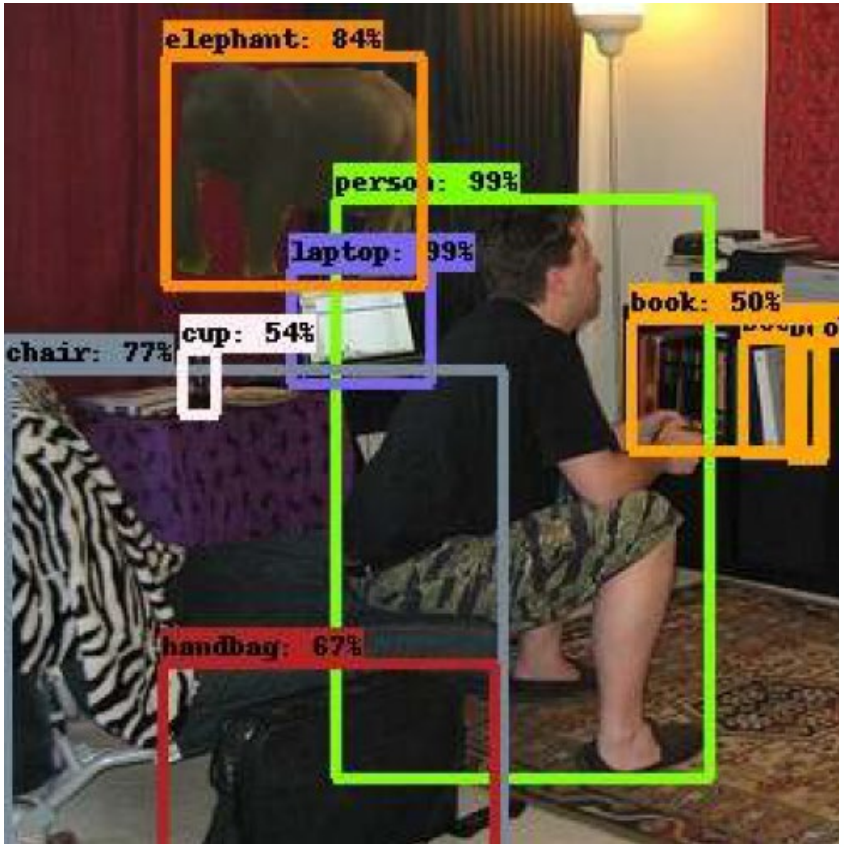





All figures on this slide taken from the reference at the top

**Rosenfeld, A., Zemel, R., & Tsotsos, J. K. (2018). The elephant in the room.** ***arXiv preprint arXiv:1808.03305*****.**

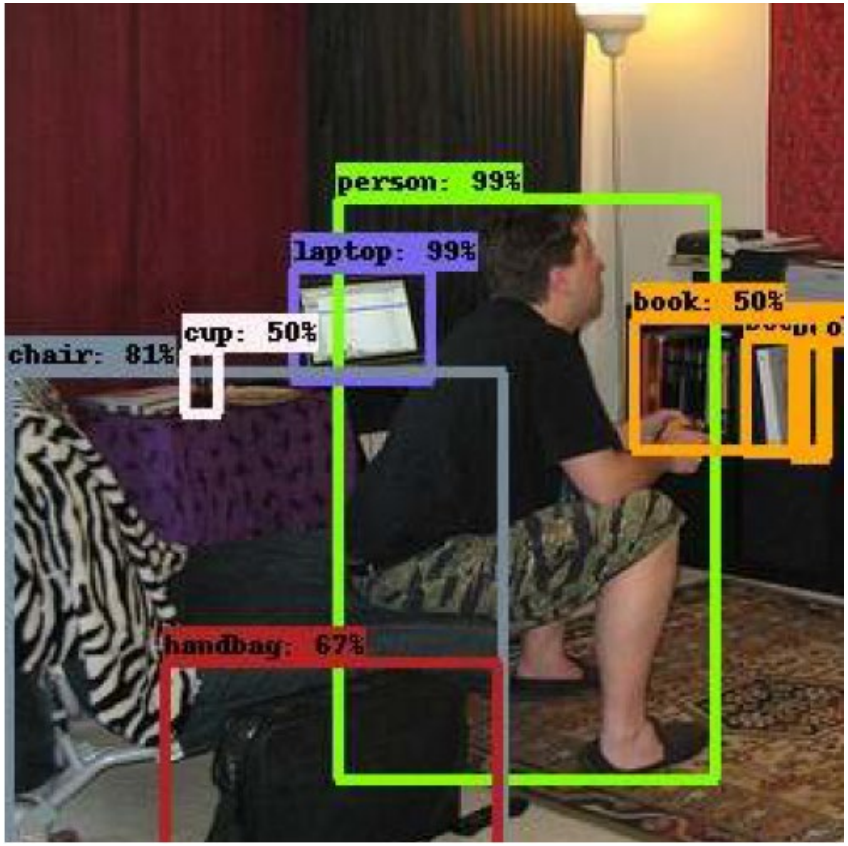


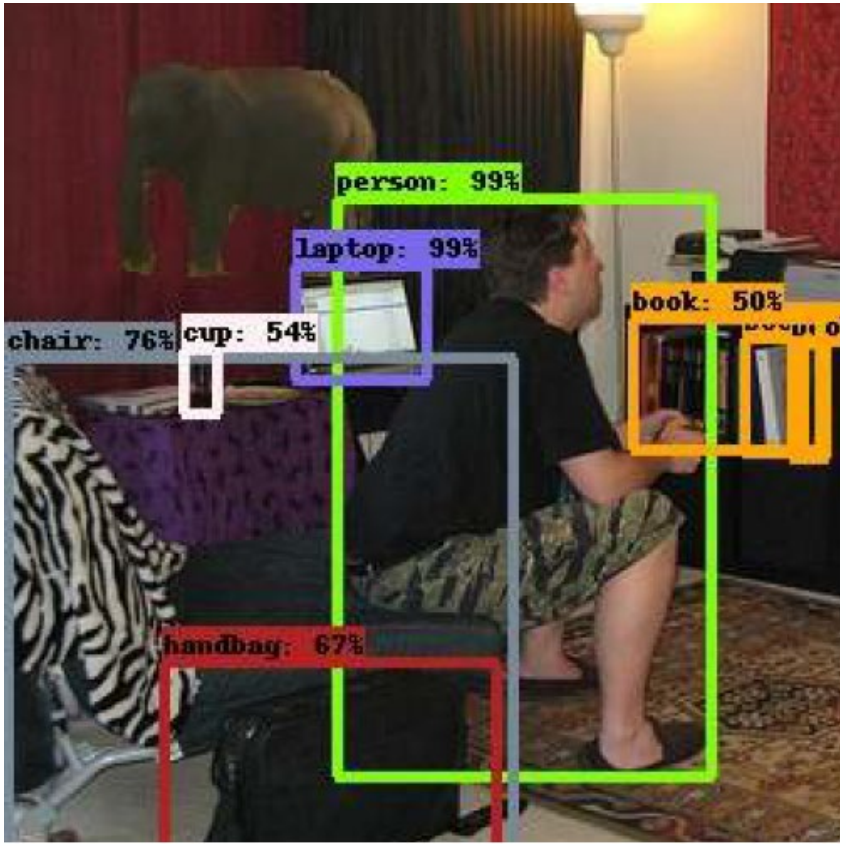






All figures on this slide taken from the reference at the top

**Rosenfeld, A., Zemel, R., & Tsotsos, J. K. (2018). The elephant in the room.** ***arXiv preprint arXiv:1808.03305*****.**






All figures on this slide taken from the reference at the top