Image Obfuscation with Quantifiable Privacy

Liyue Fan, Assistant Professor in Computer Science, UNC Charlotte

https://webpages.uncc.edu/lfan4

https://liyuef.github.io/imageprivacy/

Award #1755884 CRII: SaTC: Image Publication with Differential Privacy

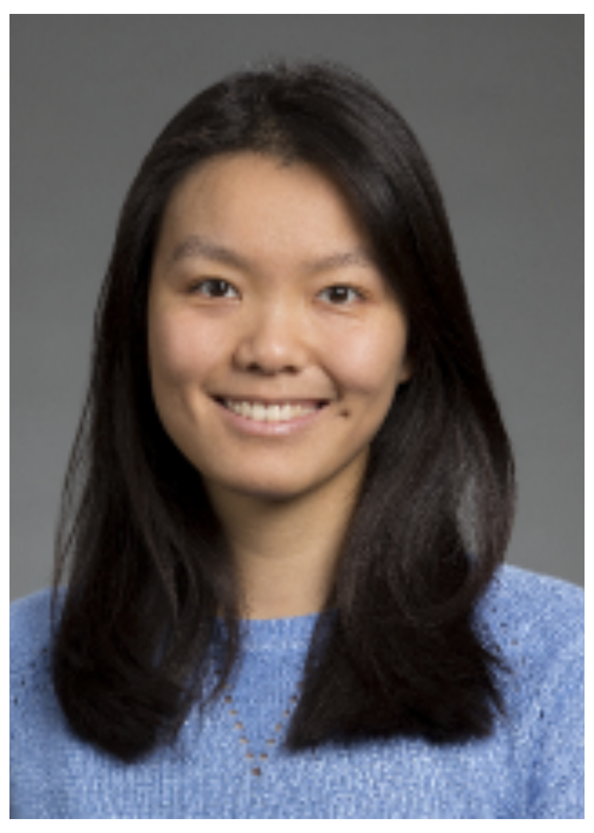
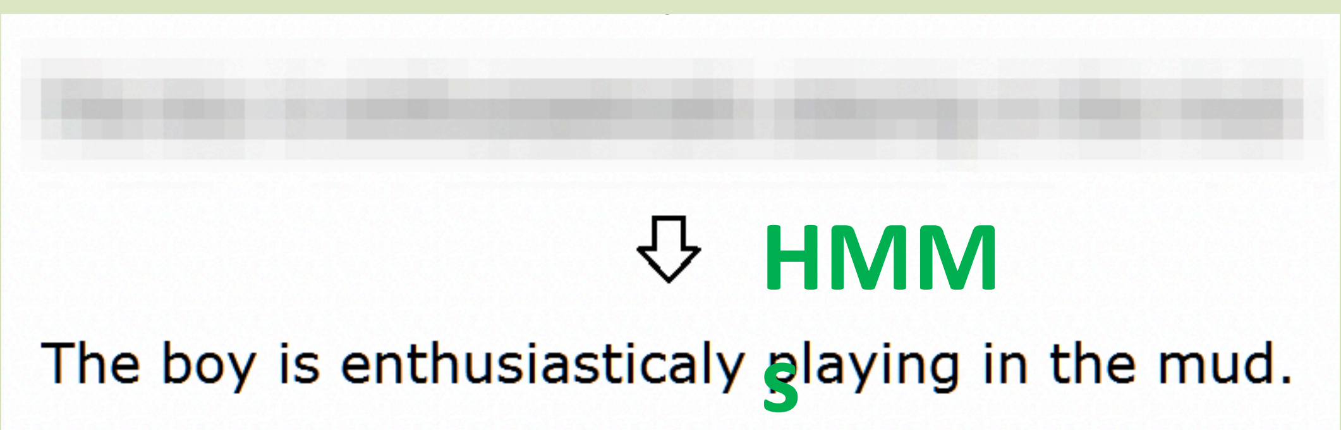


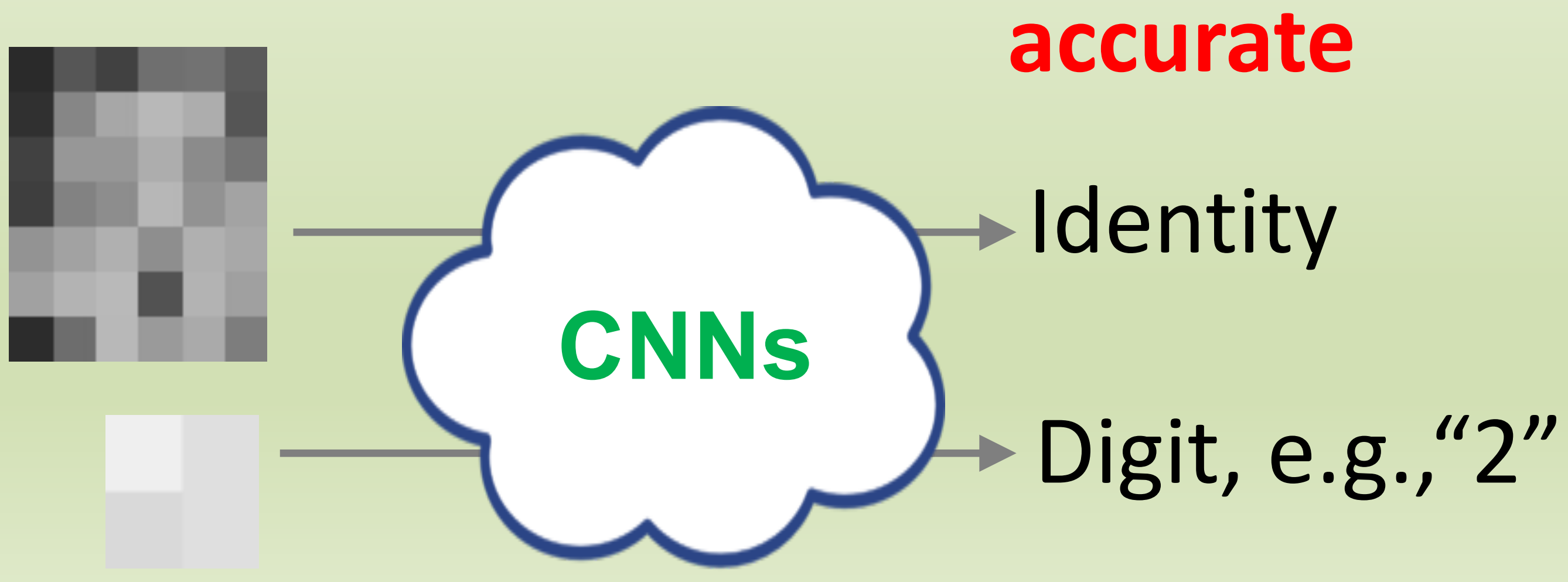
Image obfuscation is widely used to protect private content in photos, such as in Google street view [1] and journalism [2]. Some popular obfuscation techniques are blurring, pixelization, and blacking. **However,** machine learning models can *adapt to* standard obfuscation. For example:

- Hill et. al [3]



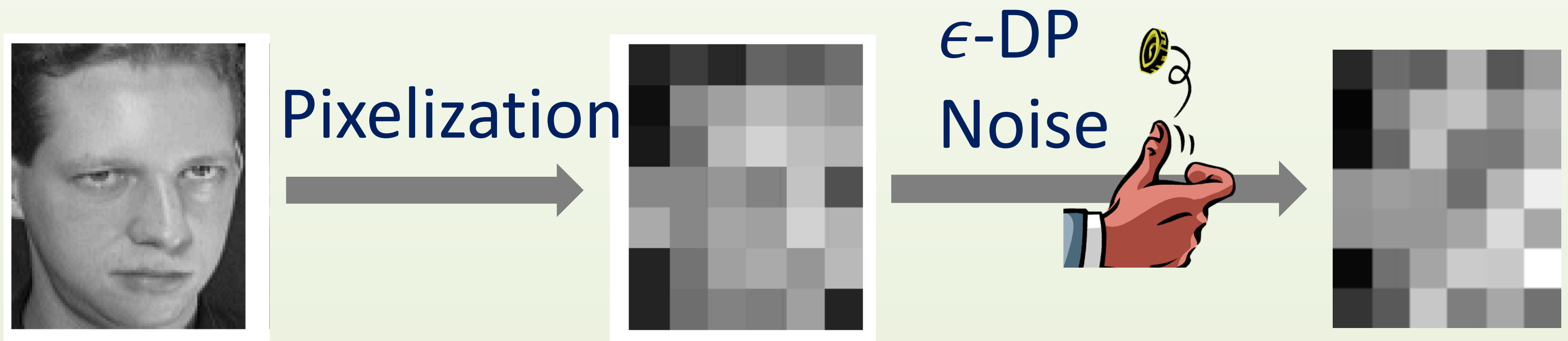
- McPherson et. al [4]

up to 96% accurate

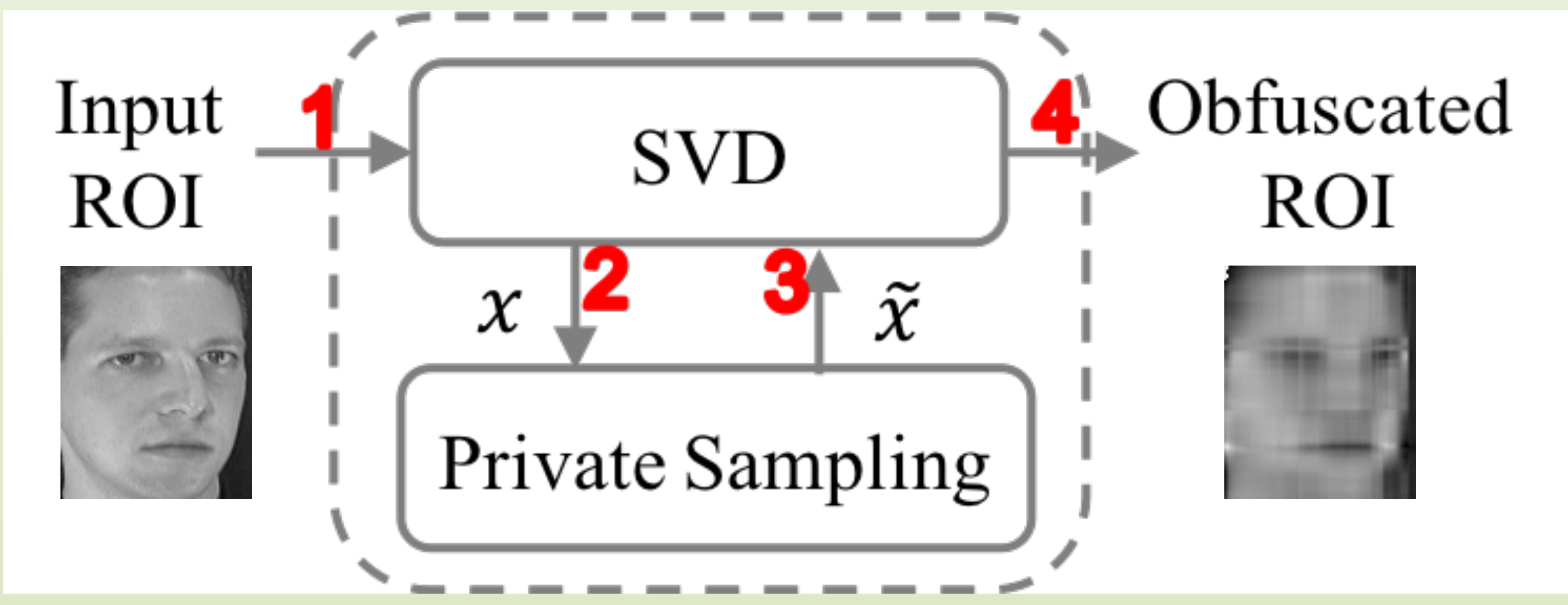


In this project, we aim at providing formal privacy guarantees, e.g., differential privacy, for obfuscating individual-level image data.

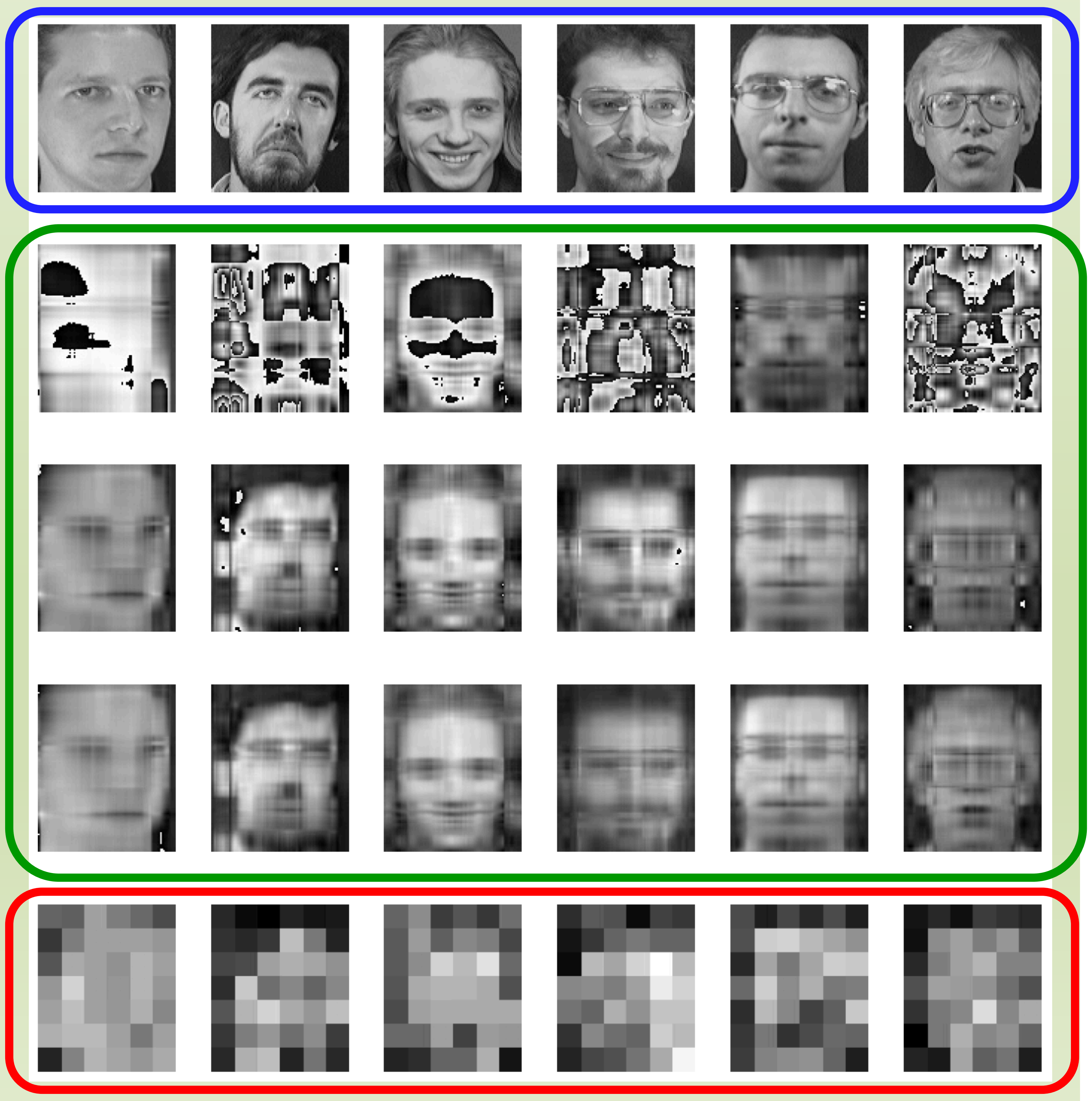
- Fan [5] achieves rigorous **ϵ-Differential Privacy** for image pixelization.



- Fan [6] improves the utility by adopting a relaxed privacy model, **metric-privacy** [7].



Results: Row 1 – original AT&T faces; Row 2 – Fan [6], ϵ = 0.1; Row 3 – Fan [6], ϵ = 0.3; Row 4 – Fan [6], ϵ = 1; Row 5 – Fan [5], ϵ = 1.



REFERENCES

1. A. Frome et al., "Large-scale privacy protection in Google Street View," 2009 IEEE 12th International Conference on Computer Vision, Kyoto, 2009, pp. 2373-2380.
2. D. Aitkenhead. `I've done really bad things': The undercover cop who abandoned the war on drugs. The Guardian, 2016.
3. Hill, S., Zhou, Z., Saul, L., & Shacham, H. (2016). On the (In)effectiveness of Mosaicing and Blurring as Tools for Document Redaction, Proceedings on Privacy Enhancing Technologies, 2016(4).
4. Richard McPherson, Reza Shokri, and Vitaly Shmatikov. Defeating image obfuscation with deep learning. CoRR, abs/1609.00408, 2016.
5. Liyue Fan. Image pixelization with differential privacy. In Data and Applications Security and Privacy XXXII, pages 148–162, Springer Cham, 2018.
6. Liyue Fan. "Practical Image Obfuscation with Provable Privacy," 2019 IEEE International Conference on Multimedia and Expo (ICME), Shanghai, China, 2019, pp. 784-789.
7. Chatzikokolakis, Konstantinos, et al. "Broadening the scope of differential privacy using metrics." International Symposium on Privacy Enhancing Technologies Symposium. Springer, Berlin, Heidelberg, 2013.

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 I Alexandria, Virginia