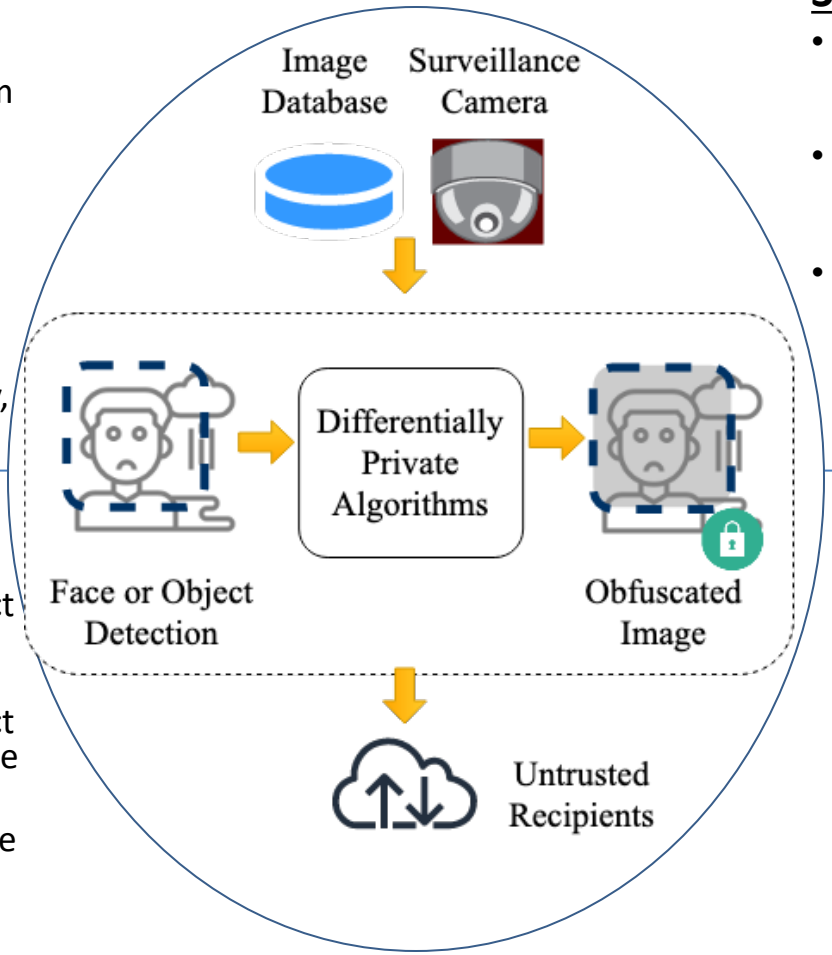
Image Publication with Differential Privacy

Challenge:

- Traditional image privacy solutions do not protect sensitive information from machine learning based inference attacks
- How to adapt differential privacy to protect image content?
- How to evaluate differentially private methods in utility, privacy, and practicality?

Solution:

- Design differentially private methods to protect sensitive content in input
- Design differentially private methods to protect features of the input image
- Design empirical privacy risk measures via inference attacks



Scientific Impact:

- Advance image privacy solutions by providing provable privacy guarantees
- Advance differentially private methods with computer vision techniques
- Advance the understanding of theoretical privacy guarantees vs. empirical privacy protection (e.g., face re-identification)

Broader Impact and Broader Participation:

- Prevent visual privacy breaches in social media, surveillance, and research data sharing
- Create software tools for broader research communities
- Provide research training to students, including those from under-represented groups

CNS 1949217: Liyue Fan, UNC Charlotte