Summary of Revision

“DP-Shield: Face Obfuscation with Differential Privacy”

We appreciate the helpful comments and suggestions provided by the reviewers. We present below a summary of changes and improvements in the revised manuscript as well as in the online demo.

1. Improvements on presentation: We updated the introduction to identify potential users interested in DP-Shields (R1). We rewrote DP preliminaries in Section 2.1 to be more descriptive, providing intuition without revealing too many technical details (R1 and R2). We removed old Figure 6 – bar charts in screenshot, because those bar charts repeat the data from Figures 2 & 3 and were less easy to read (R2). We expanded discussion on the experiment results in Section 3 (R3).
2. A new interactive component added to the demo (R3): The new component allows the audience to explore privacy methods and param values and to visualize high dimensional image embeddings in 2D space. It helps illustrate the effects of a certain privacy method/parameters on image data representation, and also provides supporting evidence for the face re-identification experiment results. We discussed this addition in Section 4.2 and presented sample visualization in the new Figure 6. The direct link to the new demo page: http://3.223.148.187/clustering
3. Planning for broader access and application (R3): currently, datasets showcased in the demo are consistent with what were discussed in the paper. However, we previously tested the methods on a number of datasets to ensure feasibility. Furthermore, we had set up a GitHub repository for code release such that the audience can explore the features of DP-Shield locally with new data. Moreover, running the code locally would allow users to apply DP image obfuscation to sensitive or personal data, which they may not send outside of trusted environments, e.g., home or secure computers.

We thank the reviewers again for the thoughtful comments that helped improve our work. We hope the changes made address the concerns raised in the initial review.