CSE 473/573 computer vision and image processing

Security issues in artificial intelligence (5% bonus homework)

The new artificial intelligence fueled by big data shows big promise in making our world more efficient, yet it could bring many issues. world Economic forum listed 9 issues of AI (https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/), including security (how do we keep AI safe from adversaries), evil genies (how do we protect against unintended consequences), humanity (how do machines affect our behavior and interactions) and artificial stupidity (how do we guard against stupidity).

Based on the recently developed free deepfake face-swapping app that is able to place your likeness into scenes from hundreds of movies and TV shows after uploading just a single photograph, please write a short essay to elaborate on the impact of AI on security. A good essay should correctly apply standard/rules considering potential consequences/conflicts, offer alternative solutions and their respective risks, and cite analogous cases as justification.

Page Limit: up to 2 pages
Due date: Dec. 09 11:59PM (late submission will not be accepted)