Style transfer for privacy preserving eye-tracking

Name: Mihir Naresh Shah
Advisor: Prof. Reynold Bailey
Agenda

- Eye tracking (background and motivation)
- Problem description
- Related work
- Proposed approach
- Milestones
- References
Eye tracking

- Record and analyse the eye images to determine where attention is focused.

**Applications:**

- VR avatars
- Attention aware interfaces
- Gaming
- Film and entertainment
- Security/authentication applications
  - Defense
  - Banking
  - E-commerce
  - Medical records

Courtesy of Pupil labs
Eye tracking images

Challenges (Motivation):

- Such applications are vulnerable to cyber-attacks because the captured eye-images encode unique biometric information.
- Eye tracking becoming more ubiquitous.
- It is essential to develop techniques that simultaneously preserve user privacy while providing real-time, accurate, and precise eye-tracking.

Figure 1 (Modified): Example from Kumar, A. and Passi, A., 2010 (p, 1016-1026).

This project explores the use of style transfer to preserve user privacy while still providing aesthetically pleasing, plausible, and functional (for eye-tracking) images of the eyes.
Related Work

- **EyeVEIL**: Uses Gaussian blur to defocus an eye image that helps improve the privacy of the user’s eye while it retains satisfactory accuracy for gaze estimation[1].

- **Rubber Sheet Model**: Uses a technique called Rubber Sheet Model transformation [John Daugman 2009]. Unlike EyeVEIL, this method does not degrade the eye image instead it replaces the iris region with a different high-quality iris texture image[2].
Proposed Approach

- **Hypothesis:** If an adversary has access to the weights of deep neural style transfer neural network then they can still reveal the user’s identity.
- After style transfer and image manipulation if iris recognition is successful then the network failed to preserve privacy.
- If it is not successful in predicting a person’s identity we then check the loss of features.
Results and Analysis

- The success of this approach highly depends on two things: Eye-tracking functionality and Identifiability

- Expected Result:
  - Low identifiability: The iris recognition algorithm fails to identify the user’s identity using the style transferred iris images.
  - Non-reversible: Given the weights of the neural style transferred model the style transferred images can not be used to generate the original image.
  - High trackability: Even after style transfer we can still preserve the important features of iris images that can be used in eye-tracking applications.
Milestones

**Milestone 1:** Reading research papers and other approaches related to Neural Style Transfer and privacy preservation of iris images, Dataset collection, setup RITnet for segmentation. Create a project report to record the progress of milestone 1.

**Milestone 2:** Implement Deep Neural Style Transfer with Privacy Preservation to generate realistic eye images and state of the art iris recognition algorithms to check if the privacy of iris patterns is preserved or not. Record the progress of milestone 2 in the project report.

**Milestone 3:** Test the entire pipeline on a larger dataset. Results and Analysis. Add the result and analysis section with future work in the project report.
References


THANK YOU