Iris Obfuscation with DCGAN

By Akhil Ghosh and Rachel Gordon

Outline

1. Introduction & Research Question
2. Dataset
3. Data Preprocessing
4. DCGAN
5. Results
6. Conclusion
7. Future Work

Introduction

Problem: Iris recognition and identification through photos posted on social media or images accessible through other sources poses a significant security risk

- It is possible to identify a person's identity based on their iris even if the image is not high quality or close-up on the eye
- There is also a lack of usable iris data in education settings in places like Europe that have laws against using data that belongs to real people

Research Objective: We want to obfuscate the irises in an image so that the person is not identifiable by this biometric data, but so that the original color and beauty of the iris is maintained

Dataset

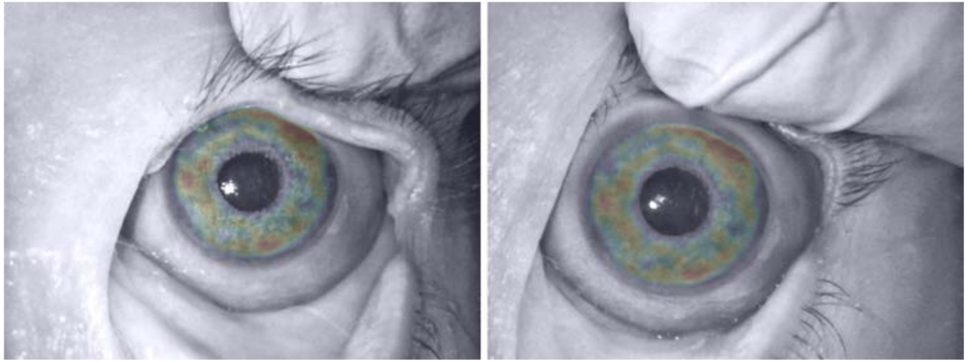
Saeed Aryanmehr, Farsad Zamani Boroujeni, October 28, 2019, "Iris Super Resolution Dataset", IEEE Dataport, doi: https://dx.doi.org/10.21227/3237-be47.

- Database of 4,320 color iris images taken from 704 subjects
  - 392 female and 312 male
- Contains three images of the left eye and three images of the right eye for each subject
- All images were taken under the same conditions and with the same color camera

Data Preprocessing

- Each image was originally 3456 x 5184
- Cropped to a square around the eye focusing the image around the iris
- Converted to grayscale and resized to 64 x 512
- Detected pupil and limbus circles
- Computed the mask to remove eyelashes
    - Only saved images that had <30% mask
- Normalized the iris to create **rubber sheet model** for GAN input
- Filled in occlusions with repeated reflections of iris segments
- Successfully preprocessed 3,164 images

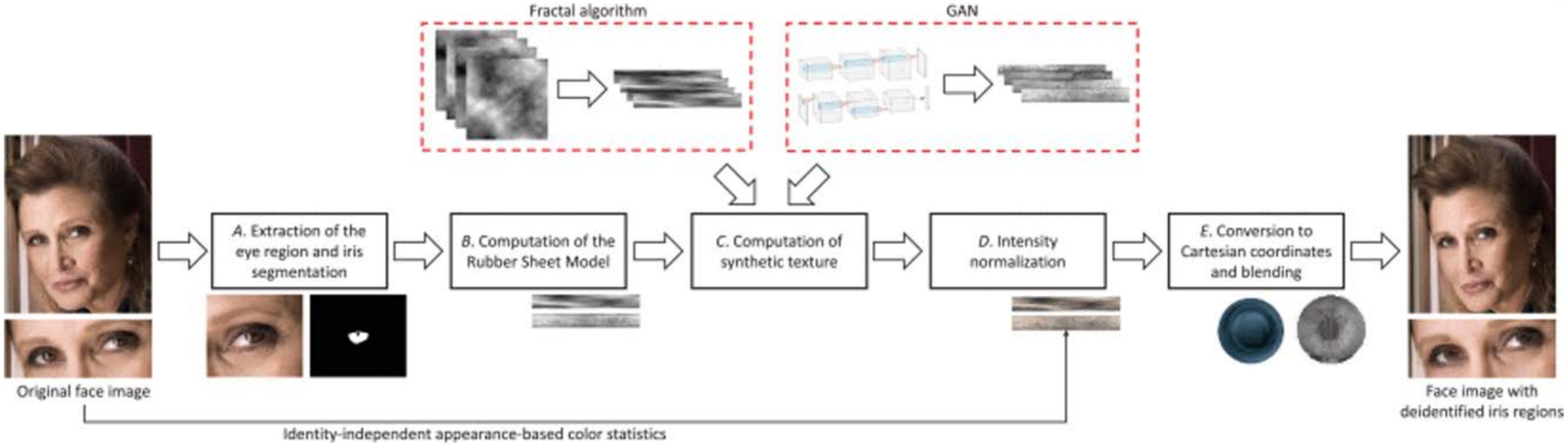
Iris Recognition



- https://github.com/aczajka/iris-recognition---pm-diseased-human-driven-bsif/tree/main
- Utilized to obtain normalized iris rubber sheets
- Also obtained masks

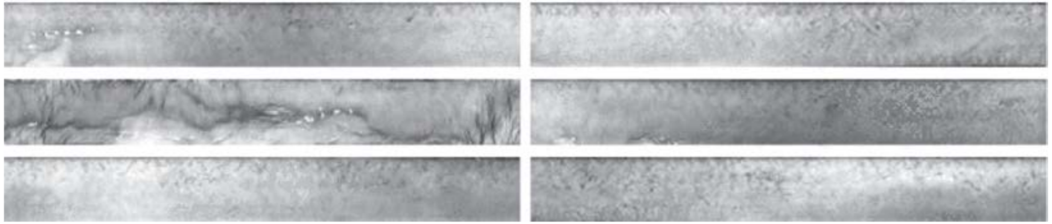
DCGAN

M. Barni, R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Iris deidentification with high visual realism for privacy protection on websites and social networks", in IEEE Access, vol. 9, 2021, pp. 131995-132010. ISSN: 2169-3536. [DOI: 10.1109/ACCESS.2021.3114588]



Results

- Example of synthetically generated iris VS celebrity iris rubber sheet (with occlusions reflected)



Color Matching

- Tried to implement a method similar to the DCGAN paper
- Applied a Gaussian filter to the generated irises
- Adjusted color intensity of each pixel value

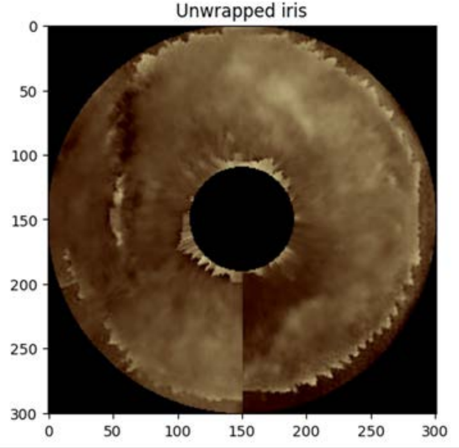
D. Color Domain Adaptation

This step aims at adapting the simulated texture T in the color domain to obtain an image C with color characteristics similar to those of the irises included in I . To perform this task, we also consider identity-independent appearance-based color statistics extracted from the iris image I but without including any biometric information originating from the real iris.

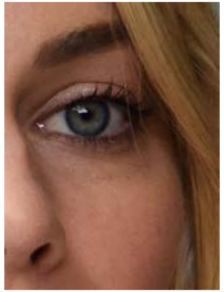
To perform the color domain adaptation, we first reduce the possible presence of visual incoherence at the extremes of T due to the transition of θ from 0 to 2π . To meet this goal, we apply a Gaussian filter to T using a kernel with an empirically estimated size of $s_k \times s_k$ pixels and with a standard deviation of σ_g . The filter is applied by considering the image T as continuous in the convolution operation, thus obtaining the smoothed image T' .

We then adapt the intensity range of
T' for each color channel of the iris region. Starting from
I and a binary mask
B representing the segmented iris, we compute a vector of intensity values
V_c , where
$c \in \{R, G, B\}$, for each of the color channels of the red, green and blue (RGB) space. We compute each channel of the color texture image
C as follows:

$$\begin{aligned} A &= T' - \text{mean}(T'), \\ C_c &= A \times [\text{std}(V_c) \times w_1 + \text{mean}(V_c) \times w_2] \\ &\quad \forall c \in \{R, G, B\}, \end{aligned} \tag{2}$$

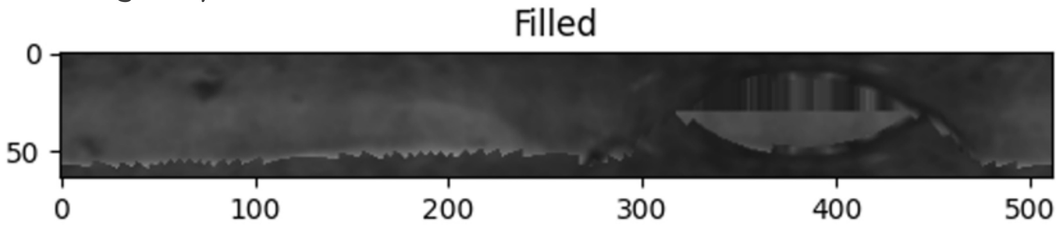


Celebrity Example



Celebrity Iris De-Identification

Right Eye



Generated Iris

Results

```
norm_iris_1 = cv2.imread('/content/righteye_im_polar_MCCNet.tiff',cv2.IMREAD_GRAYSCALE)
mask_iris_1 = cv2.imread('/content/righteye_mask_polar_MCCNet.tiff',cv2.IMREAD_GRAYSCALE)
norm_iris_2 = cv2.imread('/content/right_eye2_im_polar_MCCNet.tiff',cv2.IMREAD_GRAYSCALE)
mask_iris_2 = cv2.imread('/content/right_eye2_mask_polar_MCCNet.tiff',cv2.IMREAD_GRAYSCALE)



desc_1 = describe(norm_iris_1)
desc_2 = describe(norm_iris_2)

distance = match(desc_1, mask_iris_1, desc_2, mask_iris_2)
print('Distance:', distance)
```

```
Distance: 0.28091194014760895
```

Generate | Using ... | create a dataframe with 2 columns and 10 rows

```
[62] norm_iris_2 = cv2.imread('/content/123.jpg',cv2.IMREAD_GRAYSCALE)
     mask_iris_2 = cv2.imread('/content/right_eye2_mask_polar_MCCNet.tiff',cv2.IMREAD_GRAYSCALE)



     desc_1 = describe(norm_iris_1)
     desc_2 = describe(norm_iris_2)

     distance = match(desc_1, mask_iris_1, desc_2, mask_iris_2)
     print('Distance:', distance)
```

```
Distance: 0.5235846404677573
```

- Utilizing the GAN image, the distance increased to the point where identification no longer possible
- Distance value is as large as 2 different irises

Idealized Process/Pipeline

- Obtain NIR images of Irises
- Preprocess irises and perform transformations to cover up occlusions
- Train GAN to generate realistic normalized iris segments
- Color matching and conversion back to polar coordinates
- Replacing the original iris with the color matched synthesized iris
- Ensure that de-identification has been achieved

Conclusion

- We show that it is possible to generate synthetic irises using a GAN architecture in order to prevent iris recognition and protect privacy
- There are still issues with matching the coloring of the iris to the original image and we would like to improve this process
- Still need to implement a method for replacing the original with the synthetic iris and testing iris and facial recognition algorithms

Improvements & Future Work

- Improve code to replace occlusions so that images appear smoother
  - Could select only images that have at least 90% of the image without occlusion
- Improve color matching
- Replace iris in face image with the synthetic iris
- Test face and iris recognition on the replaced iris
- Use a larger dataset for training the model to improve performance
- Train with lower resolution iris images from face photos in addition to close-up iris data

Thank You!
Q&A