**The Impact of Bias in AI Technology: An AI Ethical Challenges and Analysis (Health Care Domain)**

Kiran Kumar Athimoolam

Nagendra Hegde

Rohit Govind

Department of Applied Machine Intelligence

College of Professional Studies, Northeastern University, Boston

EAI 6400 - Data Govern & Responsible AI

Course Number (CRN): 202425

Dr. Mimoza Dimodugno

**Introduction:**

Facial recognition technology is increasingly utilized within healthcare facilities to streamline processes, enhance security, and improve patient care. However, alongside its adoption, concerns regarding privacy and ethical implications have emerged. Reports from organizations like the National Institute of Standards and Technology have highlighted biases within facial recognition tools, particularly concerning age, gender, and race. These biases pose significant risks within healthcare settings, where inaccuracies in identification can lead to detrimental outcomes for patients.

Given these challenges, our project focuses on developing a gender classification system tailored specifically for healthcare applications. The primary objective is to accurately determine the gender of individuals depicted in medical images while prioritizing privacy preservation. By addressing biases in facial recognition technology within the healthcare domain, we aim to ensure fair and accurate outcomes across various facets of patient care.

Our project endeavors to provide a robust solution capable of overcoming the specific challenges associated with gender classification tasks within medical imaging datasets. By leveraging advanced algorithms and privacy-preserving techniques, we aim to enhance the diagnosis, treatment, and overall patient care experience within healthcare settings. Through this endeavor, we aspire to contribute to the advancement of equitable and ethical healthcare practices, ultimately benefiting patients and healthcare professionals alike.

**The Impact of Bias on AI and Ethical Concerns:**

Biases in AI technologies, particularly in facial recognition systems, can arise from multiple sources, including biased training data, algorithmic bias, or the misinterpretation of the AI's output by end-users. For example, a study conducted by Obermeyer et al. (2019) and published in "Science" revealed alarming disparities in healthcare outcomes attributed to biased AI systems. The study found that an AI system deployed in healthcare settings exhibited racial bias by systematically underestimating the health needs of Black patients compared to their white counterparts, leading to fewer referrals to care programs for Black individuals despite similar healthcare requirements. This disparity not only perpetuates existing healthcare inequalities but also underscores the profound ethical concerns surrounding deploying biased AI technologies in critical domains like healthcare. Moreover, biases in facial recognition technologies can have far-reaching implications beyond healthcare, affecting sectors such as law enforcement, employment, and education. Therefore, addressing biases in AI systems is imperative to ensure equitable outcomes and mitigate potential harms associated with algorithmic discrimination.

**Bias in health care:**

Bias in healthcare AI refers to systematic errors that can lead to unfair outcomes or discrimination against certain groups of patients. These biases can originate from various sources throughout the AI development lifecycle, from data collection to model deployment, and can significantly impact the effectiveness, equity, and trustworthiness of AI applications in healthcare. Understanding the types of bias is crucial for developing strategies to mitigate their effects and ensure that healthcare AI serves all individuals equitably.

* **Data Bias:** This occurs when the training data used to develop AI models does not accurately represent the diversity of the population. Data bias can lead to models that perform well for certain groups but poorly for others, particularly for underrepresented groups. For example, if an AI model for diagnosing skin conditions is trained predominantly on images of lighter-skinned individuals, it may be less accurate for individuals with darker skin.
* **Algorithmic Bias:** This bias arises from the algorithms themselves, even if the data is balanced. It can occur due to the assumptions made during the model development process or the choice of algorithms that may inadvertently favor certain outcomes over others. For instance, an algorithm might prioritize minimizing false positives over false negatives, which could lead to disparities in patient care.
* **Label Bias:** This happens when the labels assigned to training data reflect subjective judgments or inherent biases of those labeling the data. In healthcare, this could manifest as biased diagnostic labels that reflect historical disparities in treatment or diagnosis rates among different demographic groups.
* **Measurement Bias**: Measurement bias arises when the tools or methods used to collect data introduce errors. In healthcare AI, this could occur if the devices used to measure health indicators are less accurate for certain groups of people, leading to biased data input into AI models.
* **Reporting Bias:** This refers to the tendency to underreport or selectively report data, which can skew the information available for training AI models. In healthcare, certain conditions might be underdiagnosed or underreported in specific populations, affecting the AI's ability to recognize and treat these conditions accurately across all groups.

**Types of Bias in Facial Recognition:**

First, let us understand different kinds of biases that exist in the facial recognition system. Some common biases and their impact include:

1. **Racial Bias:** Facial recognition systems have been found to exhibit racial bias, where they are less accurate in identifying individuals with darker skin tones compared to those with lighter skin tones. This can lead to disproportionate misidentification and discrimination against individuals from racial minority groups.
2. **Gender Bias:** Facial recognition systems may also demonstrate gender bias, particularly in their ability to accurately classify individuals' gender. Studies have shown that these systems are often more accurate in classifying the gender of male faces compared to female faces, leading to disparities in recognition and representation.
3. **Age Bias:** Facial recognition systems may exhibit age bias, where they are less accurate in identifying or categorizing faces of certain age groups. This can result in misidentification or exclusion of individuals from specific age demographics, particularly older adults or children.
4. **Ethnic Bias:** Similar to racial bias, facial recognition systems may show biases based on ethnicity, leading to differential accuracy in recognizing individuals from different ethnic backgrounds. This can contribute to discrimination and unequal treatment based on ethnicity.
5. **Socioeconomic Bias:** Facial recognition systems may also reflect socioeconomic bias, where they are more accurate in identifying individuals from certain socioeconomic backgrounds compared to others. This can exacerbate existing inequalities and perpetuate social disparities.

Addressing these biases is crucial to ensure the fairness, accuracy, and ethical use of facial recognition technology across various applications and settings. This involves improving the diversity and representativeness of training data, enhancing algorithmic transparency and accountability, and implementing rigorous testing and evaluation procedures to detect and mitigate biases.

**Type of Bias addressed in this report:**

Here we are going to address the **“gender bias”** that exists in facial recognition technology and how we can try to reduce the bias and also implement privacy-preserving techniques at the same time.

Gender bias in healthcare can have significant impacts on individuals' health outcomes and experiences. This bias is more oriented towards women and causes a lot of damage when it comes to predicting their health and facial conditions.

A few examples of these biases that can impact gender particularly women are:

1. **Misdiagnosis and Delayed Diagnosis:** Gender bias can lead to misdiagnosis or delayed diagnosis of medical conditions, as symptoms may be overlooked or dismissed based on stereotypes or assumptions about gender. For example, women's symptoms of heart disease are often underestimated or attributed to other causes, leading to delayed diagnosis and treatment.
2. **Treatment Disparities:** Gender bias can result in disparities in treatment recommendations and access to care. Healthcare providers may offer different treatment options or interventions based on gender stereotypes rather than individualized medical needs, leading to unequal access to effective treatment and poorer health outcomes.
3. **Underrepresentation in Clinical Trials:** Gender bias can contribute to the underrepresentation of women in clinical trials, leading to gaps in knowledge about the efficacy and safety of medical treatments for women. This can result in the adoption of treatment protocols that are less effective or more harmful for women, as they may respond differently to medications or therapies compared to men.
4. **Reproductive Health:** Gender bias can affect reproductive health outcomes, including access to contraception, family planning services, and maternal healthcare. Women may encounter barriers to accessing reproductive healthcare services due to gender stereotypes or discriminatory practices, leading to adverse reproductive health outcomes and increased maternal mortality rates.
5. **Mental Health:** Gender bias can impact mental health diagnoses and treatment. Mental health conditions may be underdiagnosed or stigmatized based on gender norms and expectations, leading to inadequate support and treatment for individuals experiencing mental health challenges.

Addressing gender bias in healthcare requires systemic changes, including raising awareness among healthcare providers, implementing policies to promote gender equity in clinical practice and research, and ensuring that healthcare services are inclusive and responsive to the diverse needs of all individuals, regardless of gender.

**Chosen Dataset:**

Here we chose the data set that consisted of images of different age groups of both male and female gender class.

The images utilized in this project have been sourced from Kaggle. The dataset comprises approximately 10,000 facial images, each annotated with information regarding age, gender, and ethnicity. These images have been meticulously cropped and aligned for consistency.

The labels associated with each facial image are encoded within the filename, adhering to the following format: "age\_gender\_race\_date&time.jpg". For example: (100\_1\_0\_20170110183726390.jpg.chip.jpg)

Specifically:

* Age is represented as an integer ranging from 0 to 116, indicating the individual's age.
* Gender is denoted by a binary value: 0 for male and 1 for female.
* Race is represented as an integer ranging from 0 to 4, corresponding to categories such as White, Black, Asian, Indian, and Others (including Hispanic, Latino, Middle Eastern, etc.).

***\*A link to the data set has been added in the reference section of the report***

**Working with model:**

After some research, we found out different methods to implement facial recognition technology. These methods included Convolution Neural Network(CNN), Multi-layer Perception(MLP), Random Forest(RandomForest), Support Vector(SVM), etc.

But the most suitable and the more accurate model for facial recognition turns out to be CNN. Hence we implemented the CNN technique for the image processing. To summarize the implementation of the algorithm, follow the below key points:

There are 2 files with functions namely classify.py and the main file where the defined functions are called i.e. bias.py file

***\*Both the files are attached at the end of the file***

`bias.py`

* Import Statements:
  + Imports necessary libraries including `glob`, `random`, `classify`, `cv2`, `numpy`, and `classification\_report` from `sklearn.metrics`.
  + Also imports `dirname` and `join` functions from `os.path` for path manipulation.
* Image Path Setup:
  + Sets up the `image\_path` variable to point to the directory containing the images.
  + Uses `glob.glob` to collect paths to all `.jpg` files in the specified directory.
  + Sorts the image paths alphabetically.
* Data Sorting by Gender:
  + Iterates through the sorted image paths and categorizes them into lists based on gender.
  + Assumes that the gender information is encoded in the filenames, where `0` represents males and `1` represents females.
* Random Image Selection:

o Randomly selects a specified number of images from both male and female categories (2000 each in this case).

* Classification:

o Concatenates the paths of randomly selected male and female images into a single array named `imagePaths`.

o Calls the `classify.classify()` function (presumably from an external module) to perform gender classification on the selected images.

o Extracts the predicted labels and true labels from the classification results.

* Reporting:
  + Calculates and prints a classification report using `sklearn.metrics.classification\_report`, providing precision, recall, F1-score, and support for each class (gender) based on the predicted and true labels.

`classify.py`

* Import Statements:

o Imports necessary libraries including `cv2` and `os.path`.

* Function: `load\_caffe\_models()`:

o Loads a pre-trained Caffe model for gender classification.

o Reads the model architecture from the `deploy\_gender.prototxt` file and the model weights from the `gender\_net.caffemodel` file using OpenCV's `cv2.dnn.readNetFromCaffe()` function.

o Returns the loaded gender classification model.

* Function: `classify(imagePaths)`:

o Performs gender classification on a list of image paths.

o Iterates through each image path in the provided list.

o Loads the pre-trained Caffe model using `load\_caffe\_models()` function.

o Prepares the image for classification by resizing it to the expected input size (227x227) and subtracting mean values from each channel.

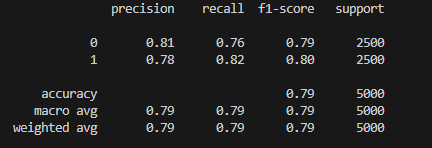
o Uses the loaded model to predict the gender of the input image.

o Appends the true gender label (extracted from the filename) and the predicted gender label to the `target` and `label` lists, respectively.

o Returns a tuple `(target, label)` containing the true and predicted gender labels for all images.

Once we developed the algorithm and implemented it we could observe that for the same amount of samples taken for both genders, we could observe the bias in the precision, recall, f1-score.

Output with bias:



**Analyzing the output and understanding the bias:**

In this output we can see that in contrast to most of the models the accuracy identifying the feature of female is better which might be a rare case. Also when we used lesser samples the bias was towards the male category and was favoring the male gender.

Let us understand the brief summary of the output as below:

From the provided classification report, we can observe the following:

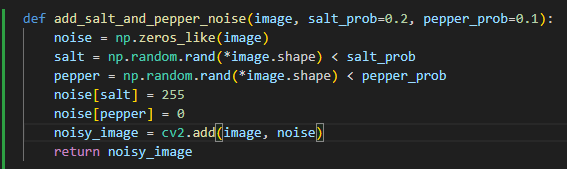
1. Precision:
   1. Precision measures the accuracy of the positive predictions.
   2. For class 0 (male), the precision is 0.81, indicating that out of all the instances predicted as male, 81% are actually male.
   3. For class 1 (female), the precision is 0.78, indicating that out of all the instances predicted as female, 78% are actually female.
   4. This suggests that the model is slightly better at correctly identifying males compared to females, but the difference is not substantial.
2. Recall:
   1. Recall measures the ability of the classifier to correctly identify instances of a class.
   2. For class 0 (male), the recall is 0.76, indicating that the model correctly identifies 76% of all male instances.
   3. For class 1 (female), the recall is 0.82, indicating that the model correctly identifies 82% of all female instances.
   4. This suggests that the model is slightly better at recalling instances of females compared to males.
3. F1-Score:
   1. The F1-score is the harmonic mean of precision and recall, providing a balance between the two metrics.
   2. For class 0 (male), the F1-score is 0.79.
   3. For class 1 (female), the F1-score is 0.80.
   4. These scores indicate a relatively balanced performance in terms of both precision and recall for both classes.
4. Support:
   1. Support refers to the number of actual occurrences of each class in the dataset.
   2. There are 2500 instances each for both class 0 (male) and class 1 (female).

Overall, the classification report indicates that the model achieves a reasonable level of accuracy, precision, recall, and F1-score for both male and female genders. However, there might be a slight bias towards classifying females, as indicated by the higher recall for females compared to males. This could suggest that the model might be better at identifying certain features or patterns in female images, leading to a higher recall score for females.

**Implementing Privacy preserving techniques to the data:**

There are several privacy preserving techniques like homomorphic encryption, Federated learning, Differential privacy, etc. Here we used Differential Privacy technique by adding salt-and-pepper noise to an image.

In this part of the code we added the noise to make sure the quality of the image remains intact but the privacy is preserved as well. We can reduce the noise or increase the needed grains to preserve the image.



Output:

Normal image Image after adding noise

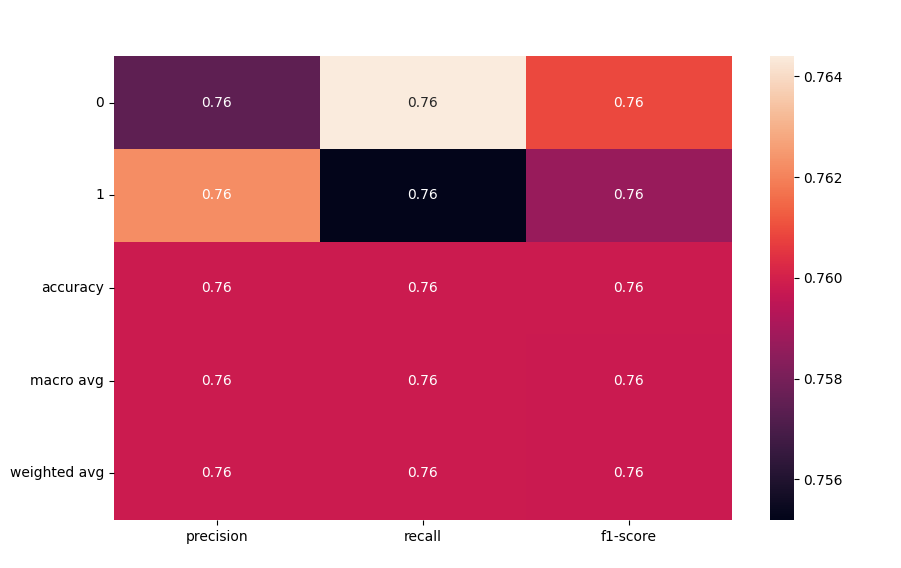
 

The output for this code can be seen in the above images where the noise has been added to the second image making it difficult to identify.

Now let us see the model output to understand if there is any impact on the bias as we have added noise to the data.

In the output below we can see that bias has been reduced. Also the accuray of the system has reduced. Here the bias has gone down tha presion, recall and f1-score are unbiased towards both the genders being at 76%.

Output:



Here are some reasons why bias might have reduced once we added the noise to the image data;

**1. Noise Regularization:** The addition of noise acts as a form of regularization, preventing the model from memorizing the training data and focusing on irrelevant features. This regularization can help reduce overfitting and improve the model's ability to generalize to unseen data, leading to a reduction in bias.

**2. Data Augmentation:** Salt and pepper noise can be viewed as a form of data augmentation, introducing additional variations in the training data. By exposing the model to a wider range of image variations, including noisy images, it can learn more robust and generalizable features, which may help reduce bias in the predictions.

**3. Fair Representation:** If the original dataset contained biases or artifacts that disproportionately affected certain demographic groups or facial characteristics, the addition of noise may have helped mitigate these biases by equalizing the representation of different groups in the dataset. As a result, the model's predictions may become more fair and unbiased.

**4. Noise-Resilient Features:** The noise added to the images may have encouraged the model to learn features that are more resilient to noise, focusing on high-level characteristics that are less sensitive to small variations introduced by the noise. This can lead to improved performance on noisy test data and a reduction in bias.

Overall, the reduction in bias and improvement in performance after adding noise to the images suggest that the noise regularization had a beneficial effect on the model's generalization ability and fairness in predictions.

**Now let us understand how can this privacy preserving technique be used in healthcare:**

Using differential privacy by adding salt and pepper noise to an image for facial recognition in healthcare offers several advantages over other encryption techniques, especially in scenarios where preserving the privacy of sensitive data like medical images is crucial. Here's why it can be considered a better option:

1. **Preservation of Image Quality:** Unlike traditional encryption techniques that might heavily distort or encrypt the image data, adding salt and pepper noise typically introduces minimal distortion to the image. This means that the image quality is preserved to a greater extent, which is important for accurate facial recognition in healthcare applications.
2. **Balanced Trade-off Between Privacy and Utility:** Differential privacy techniques aim to achieve a balance between preserving privacy and maintaining the utility of the data. By adding controlled noise to the image, it obscures sensitive details while still allowing useful features to be extracted for facial recognition tasks. Other encryption techniques might either sacrifice too much utility for privacy or vice versa.
3. **Robustness Against Re-identification Attacks:** Adding noise to the image makes it more resistant to re-identification attacks, where an adversary tries to recover sensitive information from the data. Salt and pepper noise introduces randomness that makes it challenging for attackers to reverse-engineer the original image, thus enhancing privacy protection.
4. **Compliance with Privacy Regulations:** Many healthcare regulations, such as HIPAA in the United States, emphasize the importance of protecting patient privacy. Differential privacy techniques provide a transparent and auditable way to achieve privacy compliance while still allowing for valuable analysis and research using medical image data.
5. **Ease of Implementation and Interpretation:** Implementing salt and pepper noise addition for differential privacy is relatively straightforward compared to complex encryption algorithms. It's also easier to understand and interpret the effects of adding noise to the image, making it more accessible to practitioners and researchers in the healthcare domain.

As the privacy of a patient is of the utmost importance these are some advantages that can be seen by implementing one of the privacy preserving techniques. As the filed of healthcare holds a lot of critical and personal information of an individual these encyptions are necessary to maintain the confidentiality of a person.

**Various techniques for removing the bias:**

Removing bias from AI systems and mitigating the risks associated with facial recognition (FR) technology in healthcare and other sectors involves a multi-pronged approach. Addressing these challenges requires not only technical solutions but also ethical considerations, regulatory compliance, and continuous oversight. Here are comprehensive techniques to remove bias and mitigate FR risks:

1. **Diversifying Data Sets:**
   1. Inclusion of Underrepresented Groups: Ensure training data is representative of diverse populations to prevent data bias.
   2. Synthetic Data Generation: Use synthetic data to augment real datasets, especially for underrepresented groups in training data.
2. **Algorithmic Audits and Fairness-aware Algorithms:**
   1. Regular Audits: Conduct regular audits of AI and FR systems to identify and mitigate biases.
   2. Fairness-aware Algorithms: Implement algorithms designed to minimize bias, including techniques that adjust the decision threshold for different groups or reweigh training examples to balance representation.
3. **Bias Detection and Mitigation Frameworks:**
   1. Bias Detection Tools: Use tools to detect and quantify bias in AI models based on fairness metrics.
   2. Adversarial Debiasing: Employ adversarial training methods that encourage models to learn unbiased representations of data.
4. **Explainable AI (XAI):**
   1. Transparency Tools: Implement model interpretability tools like LIME (Local Interpretable Model-agnostic Explanations) and SHAP (Shapley Additive exPlanations) to provide insights into AI decision-making processes.
   2. User-friendly Explanations: Ensure that explanations are understandable to non-experts, fostering trust and transparency.
5. **Privacy-preserving Techniques:**
   1. Anonymization and Data Masking: Use techniques to anonymize personal data, reducing the risk of privacy breaches.
   2. Federated Learning: Implement federated learning to train models on decentralized data, minimizing data privacy risks.
6. **Ethical and Regulatory Compliance:**
   1. Ethical Guidelines: Follow ethical guidelines and frameworks to ensure AI and FR technologies are developed and used responsibly.
   2. Regulatory Adherence: Comply with existing regulations like GDPR and actively engage with emerging legislation focused on AI and privacy.
7. **Continuous Monitoring and Update:**
   1. Ongoing Evaluation: Regularly re-evaluate AI systems for bias and performance issues, updating models as needed.
   2. Dynamic Consent: Implement mechanisms for dynamic consent, allowing users to control their data and opt-out of AI systems.
8. **Stakeholder Engagement and Public Awareness:**
   1. Multidisciplinary Collaboration: Engage with ethicists, sociologists, and community representatives in the development and evaluation of AI systems.
   2. Public Awareness Campaigns: Conduct awareness campaigns to educate the public on the benefits and risks of AI and FR technologies.
9. **Development of a Governance Framework:**
   1. AI Governance Bodies: Establish governance bodies to oversee the ethical development, deployment, and use of AI and FR technologies.
   2. Feedback Mechanisms: Implement feedback mechanisms to allow users to report biases or privacy concerns.

**Conclusion:**

In conclusion, addressing biases in facial recognition technology is paramount, particularly within the healthcare domain, where accurate and equitable outcomes are essential for patient well-being. Our project aimed to develop a gender classification system tailored for healthcare applications, emphasizing fair and accurate outcomes while ensuring privacy preservation.

Through an analysis of bias types and their impacts on healthcare, we identified gender bias as a significant concern, affecting diagnosis, treatment, and patient care. Misdiagnosis, treatment disparities, underrepresentation in clinical trials, and reproductive health issues are just a few examples of how bias can adversely impact healthcare outcomes.

To mitigate bias and preserve privacy, we implemented differential privacy techniques, such as adding salt and pepper noise to images. This approach offered a balanced trade-off between privacy and utility, preserving image quality while obscuring sensitive information. Importantly, it led to a reduction in bias and improved model performance, demonstrating its effectiveness in healthcare applications.

By addressing bias and preserving privacy, facial recognition technology can significantly enhance diagnosis, treatment, and patient care in healthcare settings. However, ongoing research, collaboration, and ethical considerations are essential to ensure that these technologies are deployed responsibly and ethically, safeguarding patient privacy and promoting equitable healthcare outcomes for all individuals.

In summary, our project underscores the critical importance of addressing bias in facial recognition technology within the healthcare domain. By leveraging privacy-preserving techniques and ethical considerations, we can harness the potential of facial recognition technology to revolutionize healthcare delivery while upholding patient privacy and dignity.

**References:**

Aquino, Y. S., Carter, S. M., Houssami, N., Braunack-Mayer, A., Win, K. T., Degeling, C., Wang, L., & Rogers, W. A. (2023). Practical, epistemic and normative implications of algorithmic bias in Healthcare Artificial Intelligence: A qualitative study of multidisciplinary expert perspectives. *Journal of Medical Ethics*. <https://doi.org/10.1136/jme-2022-108850>

Buolamwini, J. (2023, December 13). *Unmasking the bias in facial recognition algorithms*. MIT Sloan. <https://mitsloan.mit.edu/ideas-made-to-matter/unmasking-bias-facial-recognition-algorithms>

Buslón, N., Cortés, A., Catuara-Solarz, S., Cirillo, D., & Rementeria, M. J. (2023). Raising awareness of sex and gender bias in artificial intelligence and health. *Frontiers in Global Women’s Health*, *4*. <https://doi.org/10.3389/fgwh.2023.970312>

Chamikara, M. A. P., Bertok, P., Khalil, I., Liu, D., & Camtepe, S. (2020). Privacy preserving face recognition utilizing differential privacy. *Computers &amp; Security*, *97*, 101951. <https://doi.org/10.1016/j.cose.2020.101951>

Cirillo, D., Catuara-Solarz, S., Morey, C., Guney, E., Subirats, L., Mellino, S., Gigante, A., Valencia, A., Rementeria, M. J., Chadha, A. S., & Mavridis, N. (2020). Sex and gender differences and biases in artificial intelligence for biomedicine and Healthcare. *Npj Digital Medicine*, *3*(1). <https://doi.org/10.1038/s41746-020-0288-5>

DeCamp, M., & Lindvall, C. (2023). Mitigating bias in AI at the point of care. *Science*, *381*(6654), 150–152. <https://doi.org/10.1126/science.adh2713>

Gong, S., Liu, X., & Jain, A. K. (2021). Mitigating face recognition bias via group adaptive classifier. *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. <https://doi.org/10.1109/cvpr46437.2021.00342>

Katsanis, S. H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J. D., Evans, B. J., Lee, M. K., Anderton, J., Weinberg, S. M., & Wagner, J. K. (2021). A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PLOS ONE*, *16*(10). <https://doi.org/10.1371/journal.pone.0257923>

Latika , K., & Deepak , C. (2023). Privacy threats in facial recognition-based identity verification. *International Journal of Advanced Research in Science, Communication and Technology*, 569–572. <https://doi.org/10.48175/ijarsct-11686>

Lin, H., & Wang , R. (2022, September 15). *Anonymizing facial images to improve patient privacy*. Nature News. <https://www.nature.com/articles/s41591-022-01967-0>

Pena, A., Morales, A., Serna, I., Fierrez, J., & Lapedriza, A. (2021). Facial expressions as a vulnerability in face recognition. *2021 IEEE International Conference on Image Processing (ICIP)*. <https://doi.org/10.1109/icip42928.2021.9506444>

Salvador, T., Cairns, S., Voleti, V., Marshall, N., & Oberman, A. (2021). Bias Mitigation of Face Recognition Models Through Calibration. *ArXiv*, abs/2106.03761.

Dataset:

<https://susanqq.github.io/UTKFace/>