Systemic Review of Ethical Issues Concerning Facial Recognition

Abdulmalek Almkainzi, Abdullah M. Huwaymil, Faris A. Alhamdan, Ali S. AlDhalaan, and Abdulmalik bin Zuair.

Abstract
Facial recognition is an artificial intelligence technology used to compare a person's facial features to identify their identity. It has many applications, from identifying suspects in law enforcement to biometric identification used by many software companies today. The potential that facial recognition has for our society is extensive and could very well make our lives much safer and more straightforward. However, nothing comes without cost; even though the benefit that facial recognition may possess is excellent, it still carries plenty of ethical issues that need to be addressed; this includes the significant privacy concerns that infringe on the people's right to privacy and the possibility of misidentification when using facial recognition. This paper will go through 3 papers regarding facial recognition and examine the ethical concerns that accompany it and ways to. Resolve them.

***Index Terms*— AI ethics, Facial recognition, Ethical issues, bias in AI Facial recognition**

I. Introduction

THIS paper is a review of the literature concerning ethical issues in facial recognition AI, summarizing three papers, each with a different and unique point of view as one covers its use in health care and its ethical implications, and one takes a closer look at its use in governments and police and privacy concerns and third looks at bias in facial recognition systems and methods to mitigate and lessen its effect this paper aims to give the reader a view into the ethical landscape in facial recognition systems and bring the reader into the discussion around ethics in AI.

II. Procedures For Paper Submission

A. Review Stage

Three papers were hand-selected using google scholar and the Saudi Digital Library, two were recent and one was older, the papers had to be concerning the ethical issues and bias in facial recognition AI, each covering ethical issues in facial recognition from a different point of view the number of citations was an influential factor, the first one (What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?) [1]
Covered the topic of using Facial recognition in healthcare
The second (The ethical application of biometric facial recognition technology) [2]
Concerns about the issues of privacy
The third (Investigating Bias in Facial Analysis Systems: A Systematic Review) [3]
This is a review of the literature concerning bias in AI and ways to mitigate it.

This work is a requirement for completing the course (304) Ethical issues in computing and research methods.

The following are Students at King Saud University in the Department of Computer Science and Information Technology,

Abdulmalek Almkainzi 441170009@student.ksu.edu.sa,
Abdullah M. Huwaymil 441102592@student.ksu.edu.sa,
Faris A. Alhamdan 442102132@student.ksu.edu.sa,
Ali S. AlDhalaan 442105901@student.ksu.edu.sa,
and Abdulmalik bin Zuair 442101184@student.ksu.edu.sa.

III. First paper

(What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?) [1].

This paper focuses on the use of facial recognition in healthcare settings and its ethical implications. The author of this paper is Dr Nicole Martinez her work focuses on neuroethics and ethics regarding digital health technology.

This paper starts by giving a thorough explanation of how facial recognition works and how it could benefit health departments; researchers could utilize Facial recognition to diagnose genetic disorders, provide health information and monitor patients by using artificial intelligence to predict behaviour pain, age, and many other factors.

The paper continues to talk about consent when analyzing patients using facial recognition. Collecting consent from the patient to use facial recognition is required, but in some cases, such as machine learning where continuous input is needed, consent is not regarded as necessary, this is because to improve on the algorithm and to be able to recognize disorders. Using facial recognition to improve machine learning can lead to inaccurate bias as stated in the paper.

A concerning problem that accompanies facial recognition and the most distressing is the ethical problems in privacy. Facial recognition systems can store data as a facial images, which can be considered sensitive biometric data for patients. Few states in the USA have tried to mitigate the problem by enforcing a limit on the data collected, and HIPPA governs the handling of all biometric data to ensure that data gathered by facial recognition is safe and protected.

IV. Second Paper

(The ethical application of biometric facial recognition technology) [2] .

One of the most widely used AI (Artificial Intelligence) applications for security and law enforcement is biometric facial recognition. The use of this technology and its use have been the centre of heated debate in some nations. In 2020, it became widely known that governments were searching for suspects using information technology. The development of this technology and several related issues are discussed in the first section of the article. The second section includes significant examples from Australia, the United Kingdom, and the United States and focuses on current applications and legal developments. The decision was made to select these jurisdictions due to their earlier technology adoption. Considering these advancements, the third section of the outline moves on to conduct an ethical analysis of biometric facial recognition. On the one hand, security is looked at in terms of individual privacy, autonomy, and democratic accountability.

Biometric facial recognition is used to identify people. Using an algorithm that compares an image of a face to one that is stored in a database, a contour map of the position of facial features is turned into a digital template using a digital photograph of the subject's face. Most of the concerns about biometric facial recognition stem from the possibility of conflicts between ethical values and their application in various fields.

Biometric data is collected for law enforcement, national security, and the provision of government services, on the one hand, and for privacy and autonomy, on the other. In the absence of democratic accountability, developments in authoritarian states shed additional light on the potential consequences of biometrics.

Biometric facial recognition has seen significant applications in Australia, the United States, and the United Kingdom, and systems continue to advance rapidly. In international airports, their use in conjunction with passports, and border control systems continue to rely heavily on them, which raises the significance of this technology.

V. Third Paper

(Investigating Bias in Facial Analysis Systems: A Systematic Review) [3] .

This paper focuses on providing a systematic analysis of bias in facial analysis systems due to the perceived lack of comprehensive literature reviews on the subject and aims to identify and highlight the bias existing in public face databases and to present algorithmic solutions to this issue.

The bias can be traced in some cases to the models used and in other cases to limited training of algorithms, while in still other cases, bias can be traced to insufficient databases. To this date, no comprehensive literature review systematically investigates bias and discrimination in the currently available facial analysis software. To address the void, this study conducts a systematic literature review in which the context of facial analysis system bias is investigated in detail. The review, involving 24 studies, additionally aims to identify facial analysis databases founded to alleviate bias, to identify the various aspects of discrimination in facial analysis technology, and to recognize algorithms and techniques employed to mitigate bias in facial analysis.

The authors claimed that machine learning algorithms and the data that feed them are, at their core, a result of human-provided data and calculations; therefore, they are not exempt from reflecting human biases. Moreover, this is especially true in the case of facial analysis.

The review was conducted according to a predetermined protocol and was reported following the PRISMA Statement.

Data source and search strategy: a computerized database search was performed to identify abstracts relevant to the research topic. The strategy was applied to the following databases: Scopus, IEEE Xplore, ACM digital library, the International Prospective Register of Systematic Reviews (PROSPERO), Cochrane Database of Systematic Reviews (CDSR) and Scientific Electronic Library Online. There

were no restrictions concerning the publication's language, date or status.

The search terms were developed using controlled vocabularies and keywords. Two groups of words constituted the search strategy: (1) facial analysis; and (2) bias. The Boolean search strings in the article title or abstracts were as follows: (("face analysis" OR "facial analysis") AND (bias OR discrimination OR unfairness OR disparities)).

Selection and validity assessment:

Eligible studies should have met all the following criteria: no restrictions were imposed on the subject's age, and Ethnicity/Race, only computerized facial analysis algorithm, software or database were considered, and that standard error could be estimated from the reported values and reported values should be accurate to one decimal place, and the studies should be focused on the bias, no restrictions were imposed on language, date, and status of, the publication type was either conference proceedings or journal articles.

Studies were excluded if one or more cases from the below list were present:

1) Introduced a new facial analysis algorithm, tool or application without directly addressing the problem of bias in automatic facial analysis;

2) Exclusively reported the board and general ethical consequences of AI and Big Data use in society without directly or indirectly tackling facial analysis bias;

3) Focused on the ethical and privacy concerns of facial analysis algorithms and technology;

4) Called for algorithmic transparency as a mechanism to fight bias and discrimination without directly addressing facial analysis algorithms;

5) Studied face analysis bias where algorithms or machines did not perform the analysis and recognition.

Eligibility of the selected studies was determined by two experts in this domain, the screening was done in two rounds; the first one is a title and abstract screening and the second; is a full-text screening.

Results from the review:

The results showed that females with darker skin are the group with the highest misclassification rates (up to 34.7%), while the maximum error rate for lighter-skinned males is 0.8%. In addition, to confirming the bias and low accuracy in classifying females, other algorithmic audits reported low classification accuracy for children and young populations in general.

Our ability to perceive the different identities of other-race faces is limited to our ability to perceive the distinct identity of faces of our own race. The causes of this phenomenon can be partially attributed to social prejudices, but perceptual factors that begin to develop early in infancy were found to be the primary cause. Specifically, optimizing the encoding of unique features for the types of faces we encounter most frequently, usually faces of our race, e.g., family members—results in a perceptual filter that caps the quality of representations formed for faces that are not described well by these features. Facial analysis algorithms suffer from this effect as well. Face Recognition Vendor Test (FRVT) 2006 reported results supporting this assumption.

In the test[4], the results of eight algorithms from Western countries were fused, as were the outcomes of five algorithms from East Asian countries. The false acceptance rate, is the measure of the likelihood that the biometric security system will incorrectly grants access to an unauthorized user. Therefore, for security reasons, a low acceptance rate is usually set or chosen before utilizing a certain biometric security system. If the system does not pass the low false acceptance rate, the system will not be utilized. At the low false acceptance rates required for most security applications, the Western algorithms recognized Caucasian faces correctly more than East Asian faces, and the East Asian algorithms recognized East Asian faces correctly more than Caucasian faces. The FRVT 2006 measured performance with sequestered data Researchers concluded that the underlying causes of the "other-race" effect in people also applies to algorithms.

Three out of the eight algorithmic auditing studies examined for this survey evaluated commercial facial analysis systems as a black box with no access to the underlying algorithm. However, some of the remaining studies reported performance discrepancies between the different types of algorithms. For instance, the inclusion of healthy older adults in the training data considerably enhanced the performance of both the AAM (feature-based ML) and FAN (deep convolutional neural network) models[4]. Nevertheless, the inclusion of faces of people with dementia in the training data did not improve FAN model results, while the AAM model demonstrated significant improvement, making its performance comparable to FAN and even far surpassing it in another instance[5].

Several studies have proposed solutions to the problem of biased performance across different race and gender subgroups; studies stated that the problem of biased data could be solved either by creating datasets that are uniformly distributed across demographics or using a technique called dynamic face matcher selection. These suggested solutions are already known in the scientific community and are rather obvious. The other three techniques, however, were built specifically to address the problem of biased demographic distribution algorithmically without creating a balance or uniformly distributed dataset.

Model-based techniques: proposed the use of a decoupled classifier. Specifically, they proposed the utilization of transfer learning to mitigate the problem of having limited data on any one group. Their decoupling technique can be added on top of any black-box machine learning algorithm to learn different classifiers for different groups.

Techniques focused on the data set:

Like dynamic face matcher selection, where several face

recognition algorithms (each trained on different demographic cohorts) are accessible by a system operator, the selection of the algorithm to be utilized for classification depends on the demographic information extracted from the probe image. The group also demonstrated that training face recognition algorithms on datasets that are uniformly distributed across demographics provide consistently high accuracy across all cohorts[6]; the matching accuracy for race/ethnicity and age cohorts can be improved by training exclusively on that specific cohort.

The study concluded that some studies have demonstrated that most commercial facial analysis software and algorithms are biased against certain categories of race, ethnicity, culture, age and gender.

And that studies have further identified that the main reason for the bias is that open-source material for facial image databases, utilized in commerce and academia for training facial analysis algorithms, reflects very poor variability in these categories.

The study recommends defining a formal guide or process model for conducting facial analysis algorithmic auditing as future research topic. As the authors see this will help establish a standardized process that will encourage further research in this direction.

Also recommended investigating the effect of biased facial analysis datasets on different types of machine learning algorithms.

Another line of research could be the development of multiple-face benchmark databases that include diverse racial, ethnic and cultural differences.

VI. Conclusion

The paper summarized three papers having a unique look into the ethics of Facial recognition, and since it is a new and immerging technology that is yet to be looked at and scrutinized by the legal system and does not have clear procedures used to mitigate its side effects with regards to privacy, security and bias against cultural, racial groups and genders the authors of the paper recommend the development and research into more robust algorithms for reducing bias and a look into its effect on privacy, and taking into consideration, its medical uses. It has many applications, from identifying suspects in law enforcement to biometric identification used by many software companies today. The potential that facial recognition has for our society is extensive and could very well make our lives much safer and more straightforward.

References

[1] Martinez-Martin N. (2019). What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care? AMA journal of ethics, 21(2), E180–E187. https://doi.org/10.1001/amajethics.2019.180

[2] [2] Smith, M., Miller, S. The ethical application of biometric facial recognition technology. AI & Soc 37, 167–175 (2022). https://doi.org/10.1007/s00146-021-01199-9.

[3] [3] A. Khalil, S. G. Ahmed, A. M. Khattak and N. Al-Qirim, "Investigating Bias in Facial Analysis Systems: A Systematic Review," in IEEE Access, vol. 8, pp. 130751-130761, 2020, DOI: 10.1109/ACCESS.2020.3006051.

[4] fP.J.Phillips,F.Jiang,A.Narvekar,J.Ayyad,andA.J.O'Toole,"Another race effect for face recognition algorithms," *ACM Trans. Appl. Perception*, vol. 8, no. 2, pp. 1–11, Jan. 2011, DOI: 10.1145/1870076.1870082.

[5] B. Taati, S. Zhao, A. B. Ashraf, A. Asgarian, M. E. Browne, K. M. Prkachin, A. Mihailidis, and T. Hadjistavropoulos, ‘‘Algorithmic bias in clinical populations–evaluating and improving facial analysis technology in older adults with dementia,’’ *IEEE Access*, vol. 7, pp. 25527–25534, 2019, DOI: 10.1109/ACCESS.2019.2900022.

[6] B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge, and A. K. Jain, ‘‘Face recognition performance: Role of demographic information,’’ *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1789–1801, Dec. 2012, DOI: 10.1109/TIFS.2012.2214212.