HIGH SCHOOL EDITION
Journal of Student Research
Volume 12 Issue 3 (2023)

The Implications of Using Artificial Intelligence (AI) for Facial Analysis and Recognition

Trevor Douglas[1] and Simran Saluja[1]

[1] Rocklin High School, Rocklin, CA, USA

ABSTRACT

Many individuals have ethical concerns related to newer biometric facial recognition technologies (FRT), along with how it is being integrated into various fields of study. This paper highlights the importance of understanding the positives and negatives of this technology in today's world, particularly in terms of privacy infringement and unintentional biases in machine learning models. FRT has significant applications in healthcare, law, security, and finance. However, it raises concerns regarding privacy, data protection, and potential biases in the data and analysis. The integration of AI and machine learning in FRT introduces the risk of biased decisions and discriminatory outcomes. Overall, the implications of this research suggest that while BFRT offers valuable advantages, proper legislation is necessary to address ethical concerns and ensure the safety and privacy of individuals.

Introduction

Biometric facial recognition is a new technology that is being integrated into a multitude of careers and fields: healthcare, law, security, and even in finance. Facial recognition software is used to verify an individual's identity; and although this ability has many applications, there are ethical concerns that these applications or the use of this technology are infringing on privacy rights. In addition, many facial recognition software is based on machine learning models and artificial intelligence – which are trained using large sets of data. Oftentimes, these datasets have an unintentional bias from the creator, reflecting itself in the decisions and conclusions of the algorithm. This paper has put together knowledge regarding biometric facial recognition and artificial intelligence to understand what the positives and negatives of using this fairly new technology are in today's world.

Literature Review

What is Biometric Facial Technology?

According to Nicole Martinez-Martin, facial recognition software is often used to verify a person's identity, in a multitude of fields, including healthcare. As with any new health technology, we should be aware of the negatives of using facial recognition software. This technology raises ethical questions about privacy and data protection, potential bias in the data or analysis, and potentially negative implications for the therapeutic alliance in patient-clinician relationships. And although these are severe implications that should be kept in mind, some regulations can provide the opportunity to use this valuable piece of technology without jeopardizing the safety of patient care. Martinez-Martin explains that some of these regulations can include requiring informed consent from clinicians to patients and being open about the biases that diagnosing diseases with AI brings (*What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?*, n.d.).

Biometric facial technology trains machine learning models and artificial intelligence algorithms with large image-based datasets. In healthcare, this system is often used to differentiate patients and determine what disease they may have – helping doctors determine a prognosis. Algorithms are complex technology and can make connections between the physical traits of a person to possible diagnoses. This technology can be used to help determine if a person has a rare disease or undetectable disease (to the human eye). It is a modern healthcare miracle that can save lives (*What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?*, n.d.).

There are many concerns that biometric facial technology (BFT/BFRT) brings along with the positives. An important one that we should recognize is the conflict between the application of this technology and whether it is right ethically. According to Marcus Smith and Seumas Miller, the main ethical values that this technology questions include security, individual privacy and autonomy, and democratic accountability: the core values that any individual involved in cybersecurity is told to keep strong in any part of their work. Some argue that the technology poses a threat to individual rights by allowing for the mass surveillance of citizens in public spaces without their consent or knowledge. In some countries, it even goes as far as creating legislation allowing BFRT to be used in government and law enforcement agencies. Generally, to make sure that these new facial recognition technologies are not infringing on our rights and security. Smith and Miller dive into detail regarding this "need for regulatory frameworks to balance potential benefits of technology with the protection of individual rights and freedoms." What this means is we will need to implement proper legislation to protect individual information about the residents of the United States, and nations across the world (*What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?*, n.d.).

According to Marcus Smith and Seumas Miller, facial recognition technology helps identify individuals in real-time by using algorithms and artificial intelligence models to analyze facial features captured in images or videos. Biometric facial recognition systems are generally more reliable than traditional identification methods. For example, when compared to passwords or Private Identification Numbers (PINs), FRT takes advantage of physical characteristics in people, which are difficult to replicate (″, n.d.).

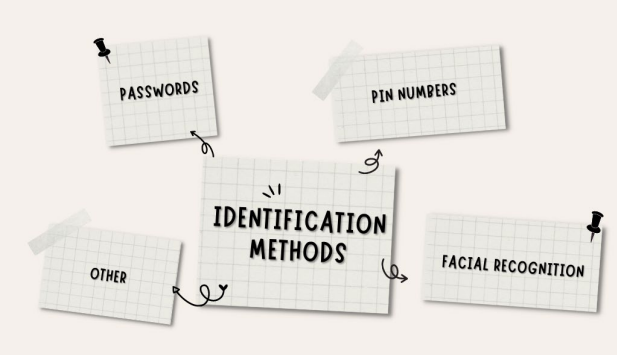

Figure 1. Types of Identification Methods.

Although this technology is more secure than passwords, for individual use at least, Smith and Miller found that private social media images have become integrated into biometric facial recognition systems. Through a study on the role of ethics in AI, it became clear that by agreeing to the mass surveillance of citizens in public spaces, without their consent or knowledge, the practical usage of FRT would pose a threat to individual rights (″, n.d.).

Some of the concerns related to facial recognition technology include accuracy (identifying people), the potential for biases, and meeting ethical expectations. Many people agree that with the increased use of artificial intelligence in FRT, there is a larger need for governance and guideline implementation to ensure that people aren't working the system and exploiting personal data. Other ethical concerns related to biometric facial recognition would include differences in decisions for whether FRT should be used in border security, criminal investigation, national security,

and private sector commercialization of data. Specifically – whether FRT uses in these domains would be a breach of personal privacy (″, n.d.).

Development over time

Since the 1960s, FRT has been in development. Early on, 2D device systems identified people from key facial features. These systems relied on manual input and had very slow speeds and accuracy as they were essentially run by people. From the 1990s onwards, 3D facial technology was developed, and this allowed for detailed facial feature analysis. In current years – the increase in artificial intelligence usage has created new opportunities for advancements in facial recognition technological use. It has also led to an improvement in the speed and accuracy of FRT when commercially used (*Facial Recognition History*, n.d.).

What is Artificial Intelligence/Machine Learning?

Artificial intelligence (AI) is a modern technological tool. AI helps people perform tasks that would require a high level of thinking & intelligence. AI can perform extreme tasks that can be difficult to perform by typical computers, for example, natural language processing, image recognition, and decision-making (″, n.d.).

To train artificial intelligence – many scientists use big data – "large datasets that are too complex for traditional data processing techniques and require advanced analytics tools and algorithms to extract insights." In facial recognition technology, artificial intelligence is trained to analyze and recognize patterns (faces and people) from visual & image-based data. AI algorithms are always first trained with a set of data before being tested with testing data. Algorithms need to be modeled with a variety of image sets to limit biases and make sure the algorithm comes to a fairly correct conclusion (″, n.d.).

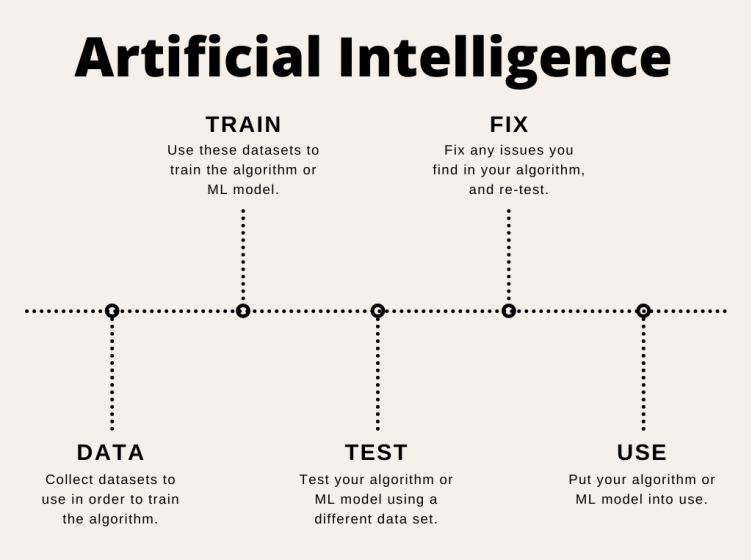

Figure 2. Steps to designing an Artificial Intelligence model.

AI and big data have applications in countless fields—including healthcare, finance, and transportation—and can improve efficiency significantly. AI can also be personalized and used for better decision-making. The use of AI in these fields, however, raises many concerns as AI can be prone to bias and discrimination. The data that artificial intelligence is trained on typically work as the sole input to the algorithm: meaning that if this data were itself biased, the program would make biased decisions as well. In terms of discrimination – the phrase "biased data leads to biased

algorithms" best explains how this occurs. If an AI model is trained with data developed by humans – the algorithm is going to have unintentional biases that reflect the creators' ethics, policies, and social beliefs (″, n.d.).

Fairness and Bias

Decisions made by artificial intelligence can have significant impacts on society, so ensuring unbiased and well-informed algorithms is integral to securing the future of AI; AI must be able to provide fair decisions—decisions that are absent of discrimination or bias (Stoychev & Gunes, 2022).

There are many different types of fairness—all of which are crucial to an unbiased algorithm. The different types of fairness in machine learning (ML) include individual fairness, group fairness, and causal fairness. Individual fairness refers to the idea that similar individuals should be treated as similar by ML models. Group fairness refers to the treatment of groups of individuals and training ML models to avoid discrimination based on characteristics that individuals within that group share. Lastly, causal fairness describes the unintentional biases rooted in past examples of bias or discrimination (Stoychev & Gunes, 2022).

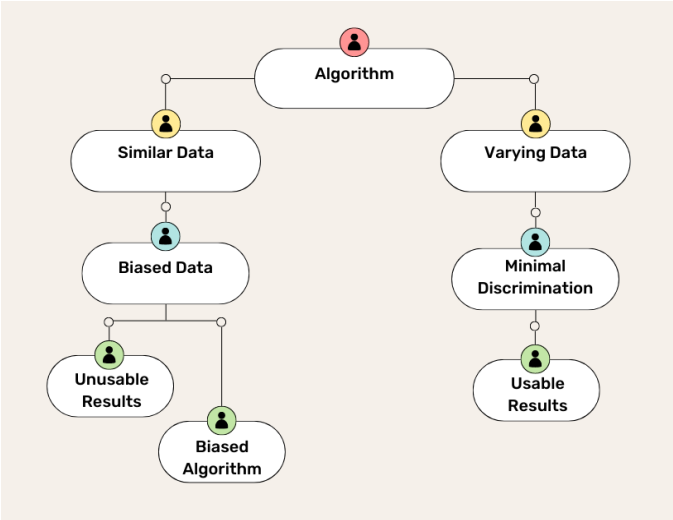

Figure 3. Comparing AI algorithms with and without varying data.

Especially when training algorithms and ML models, achieving full fairness and lack of bias is quite difficult due to the lack of diverse data. Without diverse data, models become biased to think the way they are taught instead of thinking from all possible perspectives. To completely resolve this issue, a collaborative effort must be made by all of society, working towards more accountability, transparency, and inclusivity in ML algorithms (Stoychev & Gunes, 2022).

How does Facial Recognition Technology work?

Facial recognition (FR) software is built to create a biometric profile personalized to each individual. The software analyzes facial features by capturing an image of the face and detecting specific facial landmarks—such as the eyes, nose, and mouth—and then measuring the distance between these landmarks to create a unique profile that can be used to identify an individual. Biometric templates are used to profile persons by comparing each individual to a large database with other FRT templates. This process helps governments and private companies use FRT features for security and surveillance. Specifically, it is especially used to monitor crowds for potential threats in real-time (*What Is Facial Recognition? How Facial Recognition Works*, 2021).

For example, Amazon Rekognition; is a facial recognition software designed by Amazon to identify individuals in real time from video feeds or pre-recorded content. It can be used alongside AWS (Amazon Web Services) and other applications. Some of the benefits of using such scalable applications available to the public include enhanced safety at home and increased customer satisfaction for businesses (*What Is Facial Recognition? - Face Recognition Software and Face Analysis Explained - AWS*, n.d.).

Facial recognition technology uses computer algorithms to detect, analyze, and compare facial features in digital images or video footage, according to James Andrew Lewis and William Crumpler. These features include a distance between body parts such as the eyes, nose, mouth, and forehead length, in addition to other unique characteristics to create individual profiles (*How Does Facial Recognition Work?*, 2021).

There are two main techniques when using FRT. First – geometric based, and second, feature-based. Geometric-based compares the relative positions of an individual's facial features to create a profile, whereas feature-based uses ML algorithms to identify and compare specific characteristics unique to each person (*How Does Facial Recognition Work?*, 2021).

One quite common algorithm developers use when applying FRT is the Viola-Jones Algorithm, multiple image filters that detect and analyze facial features from large datasets. Some also use neural networks which are then trained based on existing data to improve accuracy and speed. A neural network is a computer program modeled after the human brain. It includes a series of interconnected artificial neurons that provide an input based on the given data, and then provide an output. During training the neurons are provided with information, and yield a new input to other neurons or lead to the final result of the network. Then, after providing a conclusion, the network contrasts its decision with the desired decision and adjusts itself to increase its accuracy. In FRT, these networks can be trained off existing data of facial features to recognize specific aspects of individuals and recall those features when given another image of that same individual; this ability can then be personalized and used in commercial applications (*How Does Facial Recognition Work?*, 2021).

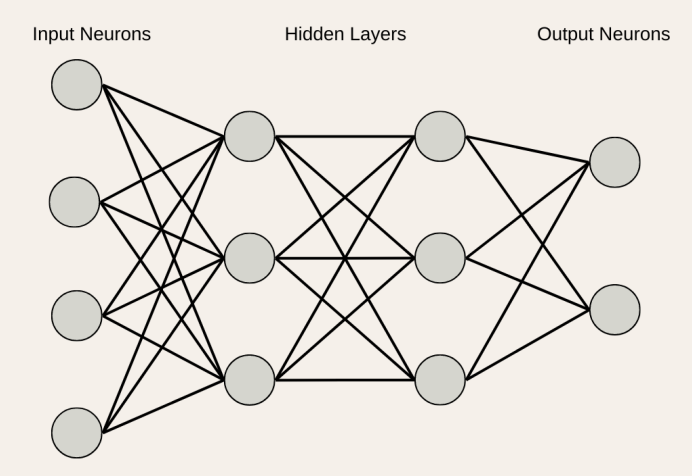

Figure 4. Showcasing a typical structure of a neural network.

FRT also uses a hardware-software combo to capture and analyze facial imagery. This process would need physical components as well, including cameras, algorithms, and a facial database. First, the developer/scientist would capture a face of a person or living being using a camera. This camera can use a combination of light types to form an image. After this, the algorithm should process the image by analyzing a multitude of key features, as mentioned previously. The features are converted into numeric code which the algorithm/ML model uses to compare large datasets and make conclusions. Accuracy can vary widely – depending on the training set that was used, the biases within the training set, the quality of testing images, the quality of the algorithm or model, and the diversity of the database

of known faces. FRT has a wide range of possible uses, but proper methods should be addressed to come to correct conclusions with the data provided (Klosowski, 2020).

Future of FRT + Proposed Bills & Regulations

FRT has recently sparked controversy and a series of ethical concerns about the software has surfaced due to its newfound popularity. The *S.2052 - Facial Recognition and Biometric Technology Moratorium Act of 2021* introduced in the U.S. Senate in March proposes a temporary prohibition on the use of FRT by federal agencies and the use of federal funds to purchase these technologies. This bill in particular aims to address privacy concerns and the discrimination controversy surrounding FRT and AI. This bill also claims to address the impacts of FRT and biometric technology use within law enforcement and provide recommendations for future limitations and policies. This bill would have a significant impact on the abilities of federal, state, and local agencies (*S.2052 - 117th Congress (2021-2022): Facial Recognition and Biometric Technology Moratorium Act of 2021*, n.d.).

Conclusion

Facial recognition technology is fairly new in today's world but has already been integrated into many different fields of study. Although FRT is useful in regard to tracking individuals and enhancing security for some, many argue new software infringes on personal rights. Some also believe that usage of this software without prior consent should not be legal – especially when it is being used in government agencies. In addition, many algorithms used to develop facial recognition software are biased due to flaws in the datasets used to train them. Overall, facial recognition software has many benefits, but the appropriate legislature should be put into place to make sure people feel safe.

Acknowledgments

Simran Saluja

First and foremost, I would like to thank my partner and co-writer Trevor, for being so helpful in the process of researching and writing about facial recognition technologies. Thank you for being so supportive! I would also like to thank my parents, Rajinder Kaur and Gurmukh Singh, for providing me with beneficial resources.

Trevor Douglas

I would like to thank my amazing co-writer, Simran, for guiding me in working on this paper and supporting me through all of the hardships that occurred. And I would also like to thank my parents, Susan Nairn and Robert Morris, for also supporting me in writing this paper.

References

″. (n.d.). ″ - Wiktionary. Retrieved June 9, 2023, from https://doi.org/10.1145/3322276.3322304

″. (n.d.). ″ - Wiktionary. Retrieved June 8, 2023, from https://doi.org/10.1007/s00146-021-01236-7

Facial recognition history. (n.d.). Thales. Retrieved June 8, 2023, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition

How Does Facial Recognition Work? (2021, June 10). CSIS. Retrieved June 8, 2023, from https://www.csis.org/analysis/how-does-facial-recognition-work

Klosowski, T. (2020, July 15). *Facial Recognition Is Everywhere. Here's What We Can Do About It.* The New York Times. Retrieved June 8, 2023, from https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

S.2052 - 117th Congress (2021-2022): Facial Recognition and Biometric Technology Moratorium Act of 2021. (n.d.). Congress.gov. Retrieved June 8, 2023, from https://www.congress.gov/bill/117th-congress/senate-bill/2052?q=%7B%22search%22%3A%5B%22Facial+Recognition+and+Biometric+Technology+Moratorium+Act+of+2021%22%5D%7D&r=1&s=1

Stoychev, S., & Gunes, H. (2022, January 5). *[2201.01709] The Effect of Model Compression on Fairness in Facial Expression Recognition.* arXiv. Retrieved June 8, 2023, from https://arxiv.org/abs/2201.01709

What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care? (n.d.). AMA Journal of Ethics. Retrieved June 8, 2023, from https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2019-02

What is Facial Recognition? - Face Recognition Software and Face Analysis Explained - AWS. (n.d.). Amazon AWS. Retrieved June 8, 2023, from https://aws.amazon.com/what-is/facial-recognition/

What is facial recognition? How facial recognition works. (2021, August 20). Norton. Retrieved June 8, 2023, from https://us.norton.com/blog/iot/how-facial-recognition-software-works#