IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Facecognizance – A ML Based Person Recognition System For Government Surveillance In Areas Under Possible Threat

Sudipta Dey[1] and Tathagata Roy Chowdhury[2]

[1.] Student, Master of Science(Artificial Intelligence), University of Huddersfield, United Kingdom
[2] Assistant Professor, Department of Computer Science and Engineering, Techno Engineering College Banipur, India

***Abstract*—**FaceCognizance, powered by machine learning (ML), revolutionizes national security with precise facial recognition and advanced threat assessment. Its ability to handle vast datasets enhances decision-making and ensures real-time adaptation to evolving threats. This proactive approach leads to faster reactions during critical situations, minimizing harm and setting a standard for responsible technological integration. However, ethical considerations, such as privacy and algorithmic biases, remain crucial. Achieving a balance between civil liberties and security measures is imperative to maintain public confidence. FaceCognizance not only advances surveillance but also serves as a benchmark for ethical ML use, reaffirming its role in shaping the future of national security.

Keywords— FaceCognizance's, surveillance, security, identification, machine learning, national security, public safety, facial recognition, ethical considerations, privacy concerns, algorithmic biases, data security, innovation, responsible technology integration.

I. INTRODUCTION

Face recognition is an important technique used in security, social networking etc. This field has seen a transformation credits to machine learning (ML). Machine learning (ML)-based face recognition systems uses complex algorithms to assess facial features by enhancing precision and consistency. These algorithms can learn patterns and subtleties from a huge datasets thatenables them to identify persons with extremely high precision. Machine Learning-based facial recognition system offers a dependable and unhindered means of identity verification.Face recognition has caused a marked change in various sectors majorly in security and social networking. This field has seen unforeseen changes and the core of this development is the useof machine learning (ML). Machine learning-based face recognition systems represent a complete change by employing detailed algorithms that dig into facial features with precision and consistency.

The fundamental strength of ML-based face recognition lies in its ability to utilize the power of complex algorithms to check facial features to utmost precision. This process enables the system to recognize patterns and subtleties embedded inside avast dataset. Thisfeature that enables it to identify individuals with exceptional accuracy. The continuous learning nature of these algorithms ensures acontinuous refinement of their understanding that allows them to adjust to diverse facial expressions, lighting conditions and other variables that ultimately enhances their precision over time.

One of the major advantages of Machine Learning-based face recognition is its capability to offer a dependable and unhindered means of identity verification. Traditional methods cannot match that level of accuracy and efficiency especially when introducedto a large volume of data. Machine Learning, however, excels in handling large datasets and can quickly and accurately identify individuals making it a important tool in various applications for secure access control systems to social media platforms.

The name of the project, "FaceCognizance: Advancing National Security through Machine Learning-Based Surveillance," was chosen to bind together the essence of its key objectives and contributions. Let's dig into a more detailed explanation of the logic behind this appropriately named initiative.

The term "FaceCognizance" is formed by "face" and "cognizance," telling us the central theme of facial recognition and the capabilities inherentedfrom machine learning. The choice of "cognizance" emphasizes a broader understanding oftell us the project's mission which is to not only to recognize faces but also to comprehend the detailed nuances within facial features. This approach aligns with the project's goal of advancing national security by surpassing simple identification to encompass a deeper understanding of patterns, anomalies and potential threats.

"Advancing National Security through Machine Learning-Based Surveillance" tells us the overarching purpose of the project. It describes the instrumental role of machine learning in elevating the efficiency of surveillance systems especially in the context of national security. By using advanced algorithms to analyze and interpret facial data this project contributes to a more sophisticated and advanced surveillance infrastructure by enhancing the ability to detect and reduce potential threats.

The careful choice of each word in the project title reflects a commitment to precision and security. "Advancing" signifies progress and improvement highlighting the project's forward-looking nature. "National Security" tells us the critical application of the technology in safeguarding the interests and well-being of a nation. "Machine Learning-Based Surveillance" emphasizes on the core technological foundation driving the project by making it clear that machine learning is not just a component but the driving force behind the initiative.

In essence, "FaceCognizance: Advancing National Security through Machine Learning-Based Surveillance" binds together a vision that extends beyond only face recognition.It symbolizes a commitment to use cutting-edge technology to fortify national security with an awareness of the ethical considerations and responsibilities that come with such advancements.

The projectaims to communicate not only its technical capabilities but also its broader societal implications. It is a proof to the potential of merging machine learning with facial recognition not just as a tool for identification but as a tool for advancing the collective security and well-being of a nation. As technology continues to move forward the initiatives like FaceCognizance set a exapmle for responsible and impactful mergingby emphasizing the transformative power of machine learning in shaping the future of surveillance and security.

The name of the project, "FaceCognizance: Advancing National Security through Machine Learning-Based Surveillance," was carefully chosen to ensure that it accurately tells its key objectives and contributions. Here's a more comprehensive explanation of the logic behind the title:

- *"FaceCognizance"*

The word "FaceCognizance" is an original and self-explaning combination of the terms "face" and "cognizance". The main objective of the research is the complex recognition and understanding of human faces and this combination highlights this goal. Different from standard monitoring techniques this approach is called "cognizance" since it suggests a higher level of understanding and analysis than just recognition.The word "FaceCognizance" emphasises a synthesis of "face" and "cognizance," binding together the project's core focus on the detailed recognition and understanding of human faces. Unlike conventional monitoring methodologies, the use of the term "cognizance" is emphasized, signifying a departure from only recognition to a more profound level of understanding and analysis. "FaceCognizance" goes beyond the normal process of facial recognition by incorporating the term "cognizance," suggesting a higher intellectual function in the system. This name signifies an ambition to achieve not only accurate identification but also a deeper comprehension of facial features, expressions and contextual nuances. The project aspires to use cognitive processesaiming for a understanding that surpasses conventional surveillance methods.

- *"Advancing National Security "*

The initiative's main objective is to significantly enhance national security. In today's complex and ever-changing threat world a nation's infrastructure, interests and population must be safeguarded by an effective security technique. By employing state-of-the-art machine learning algorithms to enhance the ability to immediately and effectively monitor potential threats and take appropriate action. FaceCognizance sets the bar in terms of national security. "Advancing National Security" serves as the critical mission of the FaceCognizance initiative acknowledging the pressing need to fortify a nation's defenses in the face of multifaceted and evolving threats. In the contemporary landscape where security challenges are dynamic and intricate the project assumes a leadership role in enhancing national security.

The sense of this objective lies in the recognition that a nation's infrastructure, interests and populace require vigilant protection. FaceCognizance emerges as a epitome by harnessing cutting-edge machine learning algorithms. These algorithms capable of processing vast datasets with unprecedented speed and accuracy empower the security tool to promptly and effectively monitor potential threats.

In today's scenario, characterized by the use of technological advancements and increasingly sophisticated threats, the importance of a proactive security approach cannot overlooked. FaceCognizance has an innovative fusion of machine learning and surveillance not only responds to this motive but also sets a benchmark for the industry. The initiative is intended to redefine the landscape of national security by providing decision-makers with actionable insights derived from advanced data analysis, thereby enabling quick and precise responses to emerging threats.

The use of state-of-the-art machine learning algorithms within FaceCognizance represents a shift in how nations approach security. It not only keeps pace with the evolving threat scenario but also recognize potential risks by offering a proactive stance crucial in safeguarding a nation's interests. By setting new standards of efficiency, accuracy and responsiveness, FaceCognizance contributes significantly to the advancement of national security measures by reinforcing the imperative for continuous innovation and adaptationin the face of ever-changing security challenges.

- *"Machine Learning-Based Surveillance"*

This portion of the title emphasizes the project's technological foundation that is machine learning. The project's use of machine learning algorithms for monitoring is one of its main points of differentiation by demonstrating its use of cutting edge technology to improve security procedures. Machine learning improves public safety by enabling the system to analyse big datasets, spot irregularities andgive decisions instantly. With a different fusion of creativity and clarity this title highlights the project's creative nature and its crucial role in advancing national security. "FaceCognizance: Advancing National Security through Machine Learning-Based Surveillance" is a summary of the project's objectives and its revolutionary contribution to the domains of surveillance and public safety. The emphasis on "Machine Learning-Based Surveillance" in the project's title is symbolism of FaceCognizance's technological process specifically its pioneering use of machine learning algorithmsfor monitoring. This strategic use of machine learning stands out as a primary differentiating feature showcasing the project's commitment to use state-of-the-art technology for the adavncement of security procedures.

Machine learning plays a pivotal role in advancing public safety. Its built-in capability to analyse vast datasets, identify anomalies and make quick decisions contributes significantly to the efficiency and effectiveness of the surveillance system. By fusing machine learning into the fabric of FaceCognizance, the project not only keeps up with technological advancements but actively harnesses them to optimize security protocols.

The chosen title "FaceCognizance: Advancing National Security through Machine Learning-Based Surveillance" perfectly captures the essence of the project. It serves as a meanto bind togetherthe multifaceted objectives and revolutionary contributions to the field of surveillance and public safety. The phrase "Machine Learning-Based

Surveillance" serves as a stalwart, representing the project's innovative approach and emphasising its pivotal role in shaping the future of security technologies. This creative fusion of advanced technology with clear objectives positions FaceCognizance as a stalwart in the intersection of machine learning, surveillance and national security.

II. BACKGROUND AND RELATED WORK

Face Recognition Technologies

Face recognition technology is classified as a biometric technology meaning that it uses specific physiological orbehavioural traits to verify and identify an individual. It emphasizes how other firms use the technology and that it is not restricted to any one company. Face recognition technology serves as a key biometric tool for identifying and verifying individuals primarily employed for monitoring and enhancing security. Its applications extend to government agencies, law enforcement and commercial sectors with numerous current uses and potential future applications. The chapter initiates with an exploration of the technology followed by an examination of some major adopters of face recognition technology on a large scale[1].

Ethical Implications of Facial Recognition

Biometric facial recognition is the name for an artificial intelligence system that automatically compares facial features.Its primary goal is to assist law enforcement in the identification of unidentified suspects through the use of pictures and closed-circuit television.Biometric facial recognition, an artificial intelligence technology, involves the automated comparison of facial features and is employed by law enforcement to identify unknown suspects through photographs and closed-circuit television. Nevertheless, the widespread adoption of this technology also brings forth notable privacy and ethical concerns that necessitate the establishment of appropriatelaws and regulations. Ethical principles are applied to address potential conflicts between security and individual privacy, autonomy and democratic accountability. This strategy strives to facilitate the establishment of appropriate laws and regulations as technology advances further.[2] It is acknowledged that in order to uncover biased system performance algorithmic auditing is required. With the best of intentions algorithmic auditing projects could have unanticipated consequences that jeopardize the populations these protections are intended to protect. Although sensitive face recognition data is handled carefully, the technology is often used in questionable ways. Despite being crucial for uncovering biased performance, well-intentioned algorithmic auditing can inadvertently inflict harm on the very populations these measures aim to protect. We outline five ethical concerns specifically related to auditing commercial facial processing technology highlighting additional design considerations and ethical tensions that auditors must be mindful of to avoid worsening or complementing the harms caused by the audited system. Furthermore, we provide concrete examples of these concerns and conclude by reflecting on the implications for the role of algorithmic audits and the inherent limitations they reveal in the products they assess[3].

Government Surveillance and Security

These days society is heavily reliant on monitoring and security. Many people install a large number of cameras in an attempt to boost security but doing so not only significantly increases costs but it also does not ensure the requisite level of protection. An Internet of Things-based face-detection and surveillance bot has been created to solve this problem and give users a higher level of comfort and security. It offers customers 360-degree surveillance and an intruder detection system (INDS) with computer vision, the Internet of Things and artificial intelligence. Its cloud-based application allows tracking of surveillance and management of bot movement. For military, residential and commercial facilities security is the top priority. It will assist in solving the main security issues for these organizations by employing surveillance and intruder detection[4]. The Face Recognition-based Smart Attendance System using IoT serves as a tool for efficiently recording student attendance by employing face biometrics through the capture of monitor camera images. The conventional method of calling out each student's name for attendance is laborious and leaves room for proxy attendance. The proposed system relies on face recognition to manage the attendance records of students. As the attendance-taking process commences, the system captures images of attendees and applies face detection and recognition techniques to identify students. Therecognized students are then marked as present and their attendance is updated with the respective time, student name and registration number. Deep learning techniques have been employed in the development of this project.[5].

Machine Learning in Surveillance

The Internet of Things ecosystem is comprised of a large number of devices, people and data. When addressing present and future "big data" problems it highlights the significance of sustainability. It also mentions that serious challenges to IoT administration arise from privacy and security. Deep learning is further enhanced in managing security concerns by incorporating principal component analysis (PCA) for feature extraction. Deep learning stands out as particularly well-suited for addressing the challenges posed by the significant data complexities and future considerations inherent in IoT. Nevertheless, ensuring security and privacy presents a crucial hurdle in IoT management. This study incorporates principal component analysis (PCA) for feature extraction, demonstrating superior performance. The primary aim of this study is to compile comprehensive survey data on various types of IoT deployments, highlighting security and privacy challenges while achieving a commendable recognition rate. The integration of the deep learning method with PCA feature extraction improves the accuracy of the process. Another key objective is to attain a high recognition rate for IoT-based image recognition in this research paper. The initial step involves investigating the application of deep learning for IoT image acquisition. Additionally, concerning IoT image registration, the research evaluates the effectiveness of the deep learning method in enhancing image recognition appropriateness with good testing accuracy. The research findings provide insights into the application of deep learning in the context of IoT.[6] Masks, scarves, sunglasses, hands on the face and other objects should not be able to completely obscure faces from recognition by algorithms used in machine learning. Our self-perception is intricately tied to our physical appearance, playing a crucial role in daily interactions, communication and routine tasks. The development of robust and accurate face recognition algorithms is essential for constructing fully automated systems capable of analyzing data from facial photographs and various methodologies are currently under exploration. In practical scenarios, these algorithms must be adept at recognizing faces even when obscured by masks, scarves, sunglasses, when hands cover the face, or when there are other items or externalsources obstructing the view. The outcomes of the proposed algorithms surpass those of existing methods, demonstrating high accuracy and a minimal loss function when applied to the suggested dataset. The suggested model, incorporating both trainable and non-

trainable parameters, performs exceptionally well. The above-average accuracy rate of 80% attests to the model's robust performance in facial recognition, marking a significant achievement. Recognizing faces from videos and photos remains of utmost importance in various applications [7].

III. PROBLEM STATEMENT AND OBJECTIVES

The main aim of the "FaceCognizance" project is to develop a smart and efficient facial recognition system that is appropriate for government surveillance operations in dubious areas by utilizing state-of-the-art machine learning techniques. The primary goal is to increase national security by streamlining the monitoring process, responding to potential threats more quickly and making the environment safer for everyone living there.

The scope of the "FaceCognizance" project is comprehensive, encompassing several key dimensions:
Advanced Facial Recognition

Enhancing facial recognition technology is the primary objective of the study. Developing an intelligent system that is capable of comprehending and evaluating emotions, behaviours and facial expressions in addition to face recognition is the aim. Better surveillance will depend on this advanced recognizing capability.

Machine Learning Integration

Using machine learning techniques to fortify the security system is part of the project's scope. As part of this, sophisticated algorithms for facial recognition, anomaly detection, predictive analytics and threat assessment must be created. The machine learning models are going to be trained on massive datasets in order to ensure superior accuracy.

Government Surveillance

Particularly for government agencies tasked with monitoring dubious regions, the initiative was created. The scope includes the installation of the system in public spaces, areas with high levels of security and important infrastructure locations. It addresses the specific needs of various agencies in order to facilitate national security protocols.

Response Time Improvement

"FaceCognizance" aims to shorten the time it takes for a reaction to potential threats. As part of the project's scope, real-time warning and monitoring systems will be created, enabling security personnel to respond promptly to suspicious activities and security breaches.

Critical issues include protecting data security, privacy and preventing algorithmic biases. The right to privacy of every individual will be protected and strict ethical guidelines will be adhered to.

"FaceCognizance" aims to spur great innovation in the surveillance space in addition to promoting national security. Within the project's scope is the dissemination of best practices as well as information, which will be encouraging additional research and development into the proper integration of emerging technology into public safety initiatives.The primary aim of enhancing national security and creating a safer environment for residents is aligned with its comprehensive objectives.

IV. METHODOLOGY

This project can be simply deployed on Android, iOS and other operating systems and it runs on widely used operating systems such as Windows, Ubuntu and Mac OS.

There are two categories for the system requirements for this project. -

Hardware Requirements

a) CPU – Any intel or AMD 64-bit or higher bit Processor.
b) RAM – 2GB (recommended)
c) Disk Space – 512 MB (recommended)
d) Capturing Device – Any high-resolution camera, web cam, recording device.

Software Requirements

a) OS – Windows 8,8.1,10 or ubuntu 18.04 LTS.

b) Software –recommended to use pycharm or other python compilers.

c) Programming Language – Python.

The below algorithm shows the implementation of the work.

Algorithm :

```
path = 'images'
images = []
classnames = []
mylist = list_files_in_directory(path)
for cl in mylist:
curimg = read_image_from_file(cl)
images.append(curimg)
classnames.append(get_filename_without_extension(cl))
end
functionfindEncodings(images):
encodelist = []
forimg in images:
img = convert_to_rgb(img)
    encode = face_recognition.face_encodings(img)[0]
encodelist.append(encode)
end
  return encodelist
end
functionmarkAttendance(name):
  with open('attandencemark.csv', 'r+') as f:
mydatalist = read_lines_from_file(f)
namelist = []
for line in mydatalist:
      entry = split_csv_line(line)
namelist.append(entry[0])
    end
if name not in namelist:
      now = get_current_datetime()
dtstring = format_datetime(now, '%H:%M:%S')
write_line_to_file(f, f'\n{name},{dtstring}')
end
end
encodelistKnown = findEncodings(images)
print('Encoding complete')
cap = initialize_webcam_capture()
while True:
  success, img = read_frame_from_webcam(cap)
imgS = resize_image(img, 0.25)
imgS = convert_to_rgb(imgS)
faceCurF = face_recognition.face_locations(imgS)
encodeCurF = face_recognition.face_encodings(imgS, faceCurF)
forencodeface, faceloc in zip(encodeCurF, faceCurF):
    # Compare face encodings with known encodings
    matches = compare_face_encodings(encodelistKnown,
encodeface)
facedis = face_recognition.face_distance(encodelistKnown,
encodeface)
matchindex = get_index_of_min_value(facedis)
end
if matches[matchindex]:
      name = get_uppercase(classnames[matchindex])
      (y1, x2, y2, x1) = faceloc
      (y1, x2, y2, x1) = scale_coordinates(y1, x2, y2, x1, 4)
draw_rectangle(img, (x1, y1), (x2, y2), (0, 255, 0), 2)
draw_filled_rectangle(img, (x1, y2-35), (x2, y2), (0, 255, 0))
```

```
draw_text(img, name, (x1+6, y2-6), 'FONT_HERSHEY_COMPLEX', 1, (255, 255, 255), 2)
markAttendance(name)
end
show_image_in_window('webcam', img)
wait_for_key_press(1)
end
```

This Algorithm implements a simple face recognition and attendance tracking system using the OpenCV and face_recognition libraries. The program begins by specifying the path to a directory containing images for face recognition. It then loads these images and extracts their corresponding class names. A function named *findEncodings* is defined to convert the images to RGB format and obtain face encodings using the face_recognition library. Another function, *markattandence*, is created to mark the attendance of recognized faces by adding their names and timestamps to a CSV file. The algorithm proceeds to encode faces from the loaded images and sets up video capture from the default webcam. In the main loop, the program continuously captures frames from the webcam, detects faces, and compares their encodings with the known encodings obtained from the loaded images. If a match is found, the program draws a rectangle around the recognized face, displays the name on the frame, and marks attendance. The processed frames are displayed in a window named 'webcam.' The program runs indefinitely, processing the webcam feed until manually terminated. Overall, this algorithm serves as a foundation for a basic facial recognition and attendance tracking system.

V. RESULTS

Data Acquisition

- Image acquisition: A high-definition camera that is installed in the classroom will be required to gather images. The system receives this image as an input.
- Dataset Creation: Prior to the identification procedure, a suspected person's dataset will be created. The purpose of the dataset creation is to train thesystem.
- Storing: The data pertaining to the suspected individual will be stored in JPG picture format.

Face recognition process

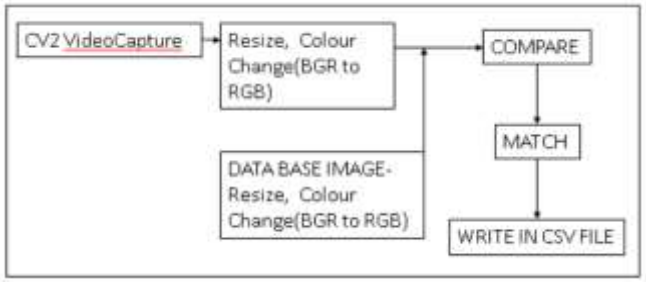


Image processing

The CV2 library runs a number of steps to process images to compare and run the facial recognition process –

Step 1: Finding all the Faces- The library uses Histogram of Oriented Gradients or HOG method in the backend for finding faces in a picture.

To detect faces in this HOG image, all what is needed to be done is to find the part of our image that looks the most resembles to a known HOG pattern that was extracted from a set of training faces:

Step 2: Posing and projecting faces

Distinct orientations look totally different to a computer:


Source:[11]

Our method entails warping every image to ensure that the lips and eyes are consistently at the sample location. This modification makes it simpler to compare faces in the following stages.

Face landmark estimation is the algorithm that will be used to do this. There are a number of ways to accomplish this, however in this instance, Vahid Kazemi and Josephine Sullivan's 2014 method will be used.

The basic idea is to pinpoint the 68 distinct locations (referred to as landmarks) that are present on each face. The upper part of the chin, the outer border of each eye, the inner border of each eyebrow, and so on are examples of these locations. The next step involves training a machine learning algorithm to identify these 68 precise spots on any face:

Here's the result of locating the 68 face landmarks on our test image:

Source:[12]

After determining the location of the mouth and eyes, all that needs to be done to get them as precisely in the center of the image is to rotate, scale, and shear it..

Step 3: Encoding Faces

The training process entails examining 3 faces simultaneously:

Load a face image of a known person from the data set.

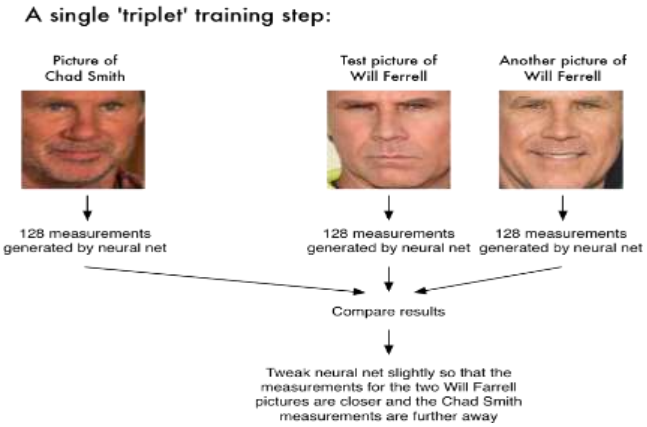
Load another picture of the same known person from the data set.

Load a picture of a completely different person from the data set

Source:[13]

In this stage, the algorithm examines the measuremen ts it is producing for each of the three photos at the mo

ment.Next, it modifies the neural network slightly to gu arantee that the measurements for #1 and #2 are som ewhat closer together while the measurements for #2 and #3 are marginally farther apart:



Source:[14]

Following millions of iterations across millions of photos of thousands of distinct individuals, the neural network learns to reliably produce 128 measures for every individual. The measurements should be roughly the same for any ten images of the same subject.

In fact, the collection of 128 measurements for each face is generally referred to as "embedding" in the context of machine learning.This idea, which involves turning complex raw data, such as an image, into a list of numerical values produced by a computer, is widely used in machine learning (particularly in language translation). The particular face methodology we use was developed in 2015 by Google researchers, while there are numerous more approaches that are similar.

VI. PRACTICES AND REGULATIONS

Common Application in Law Enforcements is that facial recognition is often used in law enforcement, which can be both positive as well as controversial depending on the specific perspective.

It highlights anumber of controversies around facial recognition that is often rooted in several concerns regarding privacy rights. We can create a number of application areas such as Automobile Security, Immigration, Access Control, Education, Retail, Healthcare and OpenAI's Contribution. It can be mentioned that OpenAI developers are contributing towards advancements in facial recognition technology.

It expresses the expectation that time will be bringing innovation to the specific use of facial recognition technology.

A impactful legislation on facial recognition must address multiple challenges simultaneously. Various facial recognition algorithms are found to be still exhibit higher error rates for African-Americans, womenand young individuals, indicating a potential reinforcement of societal biases. Beyond bias, the potent capabilities of facial recognition as a specific surveillance tool has directly led some groups for calling for a halt on its utilisation by law enforcement.Additionally, given the technology's accessible to anyone with an account of cloud developer, the private sector privacy issues are increasingly difficult to overlook which is basically leaving reformers with the question asking the approaches to fix facial recognition. Theinquiry is presented to five prominent figures representing each perspective in the policy dispute.

Facial recognition algorithms exhibit greater rate of error for African-Americans, women and young people, directly indicating all of the potential biases within the systems. It is also raising the concern that facial recognition technology might be entrenching some biases which are societal. Due to the significant power of surveillance of facial recognition, some groups advocate for a moratorium on its use by law enforcement. The respective accessibility of facial recognition technology to anyone along with a cloud developer account can be raising a number of privacy issues within the private sector. It mainly acknowledges that addressing the issues associated with facial recognition requires tackling multiple problems simultaneously[8].

VII. FUTURE DIRECTIONS

The goal of biometric systems is to measure and analyze each person's distinct physical or behavioral traits. At times, biometric systems combine certain physical features with unique attributes namely physiological (fingerprint, iris, palm print and face print) and behavioral (signature, gait, speech patterns and facial dynamics) traits. As it is non-intrusive and allows for data collection without compromising privacy, facial biometrics have emerged as one of the most popular biometric data sources. Significant historical advancements in facial biometrics are highlighted, along with important stages.It covers recent advances in face recognition through deep learning-based algorithms as well as prominent datasets used by researchers for face identification, providing insights for future dataset building methodologies [9][10]. It emphasizes how crucial it is to apply facial recognition in government surveillance in a way that upholds privacy rights and individual rights while also advancing national security.

VIII. CONCLUSION

We can identify the majority of the faces in our experiment. We recognize faces and compare them in this project using the opencv2 library.The long-term goal of the project is to turn the application into a software package with a suitable user interface and increase performance by applying the state-of-the-art facial recognition method.

REFERENCES

[1] Ian Berle, Face Recognition Technology, Law, Governance and Technology Series (LGTS, Volume 41),2020

[2]M., Smith and S., Miller, The ethical application of biometric facial recognition technology. Ai & Society, pp.1-9, 2022.

[3]Timnit Gebru, Margaret Mitchell, Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing, 2020.

[4] I,D., Raji, T., Gebru, M., Mitchell, J., Buolamwini, J., Lee and E., Denton, February. Saving face: Investigating the ethical concerns of facial recognition auditing. In Proceedings of the AAAI/ACM Conference on AI, Ethics and Society (pp. 145-151), 2020.

[5] T,S., Srinivas, T., Goutham and M.S., Kumaran, Face Recognition based Smart Attendance System Using IoT, 2022.

[6] I.J., Jacob and P.E., Darney, Design of deep learning algorithm for IoT application by image based recognition. Journal of ISMAC, 3(03), pp.276-290, 2021.

[7] R.K., Shukla, A.S., Sengar, A., Gupta, A., Jain, A., Kumar and N.K., Vishnoi, December. Face Recognition

using Convolutional Neural Network in Machine Learning. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 456-461). IEEE, 2021.
[8] L., Barrett, Ban facial recognition technologies for children-and for everyone else. BUJ Sci. & Tech. L., 26, p.223, 2020.
[9] M., Taskiran, N., Kahraman and C,E., Erdem, Face recognition: Past, present and future (a review). Digital Signal Processing, 106, p.102809, 2020.
[10] H.E.Y.D.I., MÉNDEZ-VÁZQUEZ, Y.O.A.N.N.A., MARTÍNEZ-DÍAZ and M.I.G.U.E.L., GONZÁLEZ-MENDOZA, A study on the performance of unconstrained very lowresolution face recognition: Analyzing current trends and new research directions. IEEE Access, 9, pp.75470- 75493, 2021.
[11]https://miro.medium.com/v2/resize:fit:828/format:webp/1*x-rg0aSpKOer1JF-TejYUg.png ,2016
[12]https://miro.medium.com/v2/resize:fit:828/format:webp/1*xBJ4H2lbCMfzIfMrOm9BEQ.jpeg ,2016
[13]https://miro.medium.com/v2/resize:fit:828/format:webp/1*igEzGcFn-tjZb94j15tCNA.png ,2016
[14]https://miro.medium.com/v2/resize:fit:828/format:webp/0*Vj-KASnVZ4a7B343 ,2016