

**Project Report on**

**Verification of Test-Taker**



### PG-Diploma

in

## Big Data Analytics

From **C-DAC ACTS (Bangalore)**

## Guided by:

## Miss. Sukeshini Ramadasu

##### Presented by:

Mr. Akash Singh PRN: 23035012500 6 Mr. Rishikesh Bachhav PRN: 230350125017

##### Mr. Sahil Rahate PRN: 230350125071



# Candidate’s Declaration

We hereby certify that the work being presented in the report titled: **Verification of Test-Taker**, during Post Graduate Diploma in Big Data Analytics and submitted to the department of PG-DBDA of the C-DAC ACTS Bangalore, is an authentic record of our work carried out during the period, 30th July 2023 to 30th August 2023 under the supervision of Miss. Sukeshini Ramadasu, C-DAC Bangalore. The matter presented in the report has not been submitted by us for the award of any degree of this or any other Institute/University.

Name and Signature of Candidate:

Mr. Akash Singh PRN: 230350125006 Mr. Rishikesh Bachhav PRN: 230350125017 Mr. Sahil Rahate PRN: 230350125071

Counter Signed by:



CERTIFICATE

TO WHOMSOEVER IT MAY CONCERN

This is to certify that

##### Mr. Akash Singh

##### Mr. Rishikesh Bachhav

Mr. Sahil Rahate

Have successfully completed their project on

**Verification of Test-Taker**

**Under the guidance of**

Miss. Sukeshini Ramadasu

Miss. Sukeshini Ramadasu Mr. Sanjay Adhiwal (Project Guide) (Project Co-ordinator)



# Acknowledgement

We take this opportunity to express our gratitude to all those people who have been directly and indirectly with us during the competition of this project. we pay thanks to **Miss. Sukeshini Ramadasu** who has given guidance and a light to us during this major project. Her versatile knowledge about “**Verification of Test-Taker**“ has eased us in the critical times during the span of this Final Project. We acknowledge here out debt to those who contributed significantly to one or more steps. We take full responsibility for any remaining sins of omission and commission.

Students Name

Akash Singh

Rishikesh Bachhav Sahil Rahate



Contents

[Abstract 6](#_TOC_250002)

1. [Introduction and Overview 7](#_TOC_250001)
2. Dataset 9
3. Materials and Methods 10
4. Model Building 12
5. Conclusion 14
6. Applications 15
7. System and Software Requirements 16
8. References 17



## Abstract

The project revolves around the Verification of Test Takers through the exclusive use of facial recognition technology, a pivotal task at the crossroads of modern biometrics and educational assessment. By harnessing the capabilities of state-of-the-art facial recognition algorithms, the project establishes a robust framework for verifying the identities of test takers securely and efficiently. The multifaceted challenge encompasses not only the technical intricacies of facial recognition but also the ethical implications of biometric data usage in educational settings. The primary goal is to design and implement a comprehensive system that seamlessly integrates facial recognition, ensuring the authenticity of test-taker identities while upholding privacy rights. The significance of the project lies in its potential to revolutionize the way assessments are conducted in online and remote environments, mitigating the risks associated with impersonation and dishonesty. Through the facial recognition model and its integration into the assessment process, the project aims to establish a thorough understanding of the system's accuracy and limitations, culminating in a practical and effective solution for identity verification in educational assessments.



## Introduction and Overview

In a realm where humans effortlessly craft descriptions for images, computers have struggled to replicate this innate ability. Similarly, in the context of verifying test takers, harnessing technology for precise identity confirmation presents a significant challenge. The project's focus on facial recognition as an authentication method intersects the advancements in biometrics and educational assessment. This project aims to seamlessly verify test takers' identities by capturing their facial images through the camera and matching them against a pre-established database. This juncture of biometrics, computer vision, and education aligns with the need for robust, accurate, and ethical identity verification mechanisms in remote assessments. By bridging the gap between human perception and technological authentication, our project endeavors to enhance the integrity and security of online evaluations, ensuring that the digital realm remains a trustworthy platform for educational endeavors.

Understanding the Objective and Project Flow

The primary objective of this project is to design, develop, and implement a facial recognition-based identity verification system for test takers in online assessments. The aim is to harness the capabilities of facial recognition technology to ensure the authenticity of individuals attempting tests remotely. By seamlessly integrating biometric authentication, the project seeks to address the critical challenge of maintaining the integrity and security of educational assessments conducted in virtual environments. The ultimate goal is to provide educational institutions with a reliable and efficient mechanism to verify the identity of test takers, mitigating the risks associated with impersonation and fraudulent activities.

Project Flow:

The project encompasses a well-defined flow that navigates through the stages of capturing facial images, processing and matching them, and providing verification results. The project's flow can be divided into several key steps:

Camera Initialization: The process commences with the initialization of the camera, enabling the capture of the test taker's facial image. The camera setup is crucial to ensure high-quality images for accurate recognition.

Facial Image Capture: Once the camera is activated, the system captures the facial image of the test taker. This image serves as the input for the subsequent recognition process.



Database Comparison: The captured facial image is then compared against a database containing authorized test takers' reference images. This comparison involves advanced facial recognition algorithms that analyse key facial features.

Recognition and Verification: The comparison results in a recognition score or a match probability. If the score meets a predefined threshold, the system verifies the test taker's identity, confirming their authenticity.

Result Reporting: The final step involves reporting the verification result. If the test taker's identity is successfully verified, the system communicates this outcome to the assessment platform. In cases of non-verification, appropriate actions can be taken, such as manual review or follow-up authentication methods.

Throughout the project flow, careful attention is given to optimizing the accuracy and speed of facial recognition, ensuring that the system seamlessly integrates with the assessment process. The project's success hinges on the synergy between technical precision, user-friendliness, and ethical considerations, resulting in a robust and effective solution for identity verification in online assessments.



## Dataset

In this project, the dataset plays a pivotal role as it forms the foundation for training and evaluating the facial recognition system. The dataset comprises photographs of project participants and their classmates, collected for the purpose of identity verification. This personalized approach enhances the relevance and authenticity of the dataset, closely simulating real-world scenarios encountered in educational assessments. By utilizing familiar faces, the dataset mirrors the diversity of test takers and encapsulates the variations in facial features, expressions, and lighting conditions that occur naturally.

**Dataset and Data Management:**

The dataset creation begins with the collection of facial images from project participants and their classmates. Consent and ethical considerations are paramount during this phase, ensuring compliance with data protection regulations and safeguarding privacy.

**Data Collection and Preprocessing:**

The process of dataset creation commences with the collection of passport-size facial photographs from project participants and their friends. This collection adheres to consent and ethical considerations to ensure participant privacy and data protection.

Before integration into the system, collected photographs undergo meticulous preprocessing steps. Each image is resized to a standardized 216 x 216 resolution, optimizing the dataset for recognition accuracy while maintaining proportional integrity.

**Data Storage:**

The processed facial images find their repository in a Firebase NoSQL database, chosen for its adaptability, scalability, and efficient handling of unstructured data. This database architecture accommodates resized images facilitating seamless retrieval and management. Stringent data security and privacy measures are pivotal during database management, with encryption and access controls in place to safeguard sensitive information and prevent unauthorized access.



## Materials and Methods

This section outlines the materials used and the methods employed in the implementation of the facial recognition-based identity verification system. It provides a comprehensive overview of the hardware, software, and tools utilized, along with the step-by-step procedures adopted to achieve the project's goals.

**3.1.1 Hardware and Software:**

The project's implementation required the following hardware and software components:

**Hardware:**

* Webcam or camera: A high-quality camera was employed to capture facial images.
* Computer system: A computer with sufficient processing power and memory to run the facial recognition algorithms effectively.

**Software:**

* Python: The primary programming language used for implementing the facial recognition system.
* OpenCV: A powerful open-source computer vision library in Python used for image capture, preprocessing, and facial recognition.
* Firebase: A cloud-based database platform utilized to store and manage the dataset.
* Data Preprocessing Tools: Image processing libraries and tools used to resize, normalize, and augment the facial images.

**Methods:**

The implementation of the facial recognition-based identity verification system involved several key steps:

**Data Collection:**

Passport-size photographs of project participants and their friends were collected under controlled lighting conditions to ensure image quality.

Consent was obtained from participants, adhering to ethical considerations and data protection regulations.

**Data Preprocessing:**

Collected images were resized to a standardized 216 x 216 resolution to maintain uniformity.

Image preprocessing techniques, including normalization and alignment, were applied to enhance recognition accuracy.

**Database Setup:**

Firebase was chosen as the NoSQL database platform to store processed facial images.

**Facial Recognition Model:**

A suitable facial recognition model, such as a pre-trained neural network, was selected.



**Verification Process:**

During the verification process, the webcam captured the facial image of the test taker.

The facial recognition model compared the image with the reference images stored in the Firebase database.

**Result Reporting:**

The verification result—whether the test taker's identity was successfully verified—was reported to the assessment platform.

If the verification failed, appropriate actions, such as manual review or additional verification methods, can be initiated.

**Ethical Considerations:**

Throughout the process, ethical principles were maintained, including participant consent, data privacy, and compliance with regulations.

The project's methods combined the power of computer vision, machine learning, and cloud-based data management to achieve the goal of accurate and secure identity verification. The integration of these methods facilitated the development of a robust and effective system, capable of enhancing the integrity of online assessments.

Top of Form



1. Model Building

The construction of an effective facial recognition model is a pivotal aspect of the project, enabling accurate and reliable identity verification. This section outlines the steps involved in building the model, considering the utilization of a pre-trained facial recognition model, data preparation, and integration into the identity verification system.

**Pre-trained Model Selection:**

Leveraging a pre-trained facial recognition model expedites the development process while benefiting from the model's learned features.

**Labeling and Encoding:**

Each image is labeled with the corresponding identity, enabling the model to learn associations between images and labels.

**Feature Extraction:**

For each facial image, the pre-trained model is used to extract a feature vector that captures the unique facial characteristics.

**Deployment and Integration:**

The pre-trained model is integrated into the identity verification system, where it forms the core of the facial recognition component. It takes captured facial images as input, extracts features, and performs comparisons to verify identities.

**Benefits of Pre-trained Models:**

* Feature Learning: Pre-trained models capture intricate facial features from massive datasets, making them adept at extracting meaningful representations.
* Time and Resource Efficiency: Utilizing a pre-trained model reduces the time and computational resources needed for training from scratch.
* Robustness: Pre-trained models have learned features across diverse scenarios, enhancing robustness and adaptability.

**Model Overview:**

The model employs a pre-trained facial recognition algorithm, integrated with OpenCV and the face\_recognition library. Captured images are preprocessed, and the model's feature extraction prowess is harnessed to match the image against a Firebase-stored database. Successful verification triggers identity confirmation, enhancing the security and trustworthiness of online assessments. This technically adept approach ensures seamless integration and continual adaptability for robust identity verification.

In summary, the integration of a pre-trained facial recognition model streamlines the model building process, providing accurate and efficient identity verification. The trained model's seamless integration into the verification system encapsulates the project's core objective of enhancing the security and integrity of online assessments.



**Overview of the face\_recognition Python Library:**

The face\_recognition library is a powerful tool for facial recognition tasks within Python. Built upon dlib's deep learning capabilities, it provides a user-friendly interface to work with facial recognition functionalities. The library simplifies the process of detecting, extracting, and comparing facial features, making it accessible for various applications, from security to creative projects.

**Key Features:**

**Face Detection:**

* The library can locate faces within images or video frames using sophisticated algorithms.
* It accurately identifies face positions, even when faces are at different angles or under varied lighting conditions.

**Facial Landmark Detection:**

* face\_recognition can identify facial landmarks like eyes, nose, and mouth.
* This capability is crucial for accurate face alignment and feature extraction.

**Face Encoding:**

* The library extracts unique feature vectors, or face encodings, from detected faces.
* These encodings are used for recognition and comparison tasks.

**Face Recognition:**

* The extracted face encodings facilitate comparing faces against known references.
* It allows for recognition within databases and verification scenarios.

**Simple API:**

* The library offers a straightforward API for implementing facial recognition functionalities.
* Users can quickly integrate these features into their projects without extensive coding.

**Speed and Efficiency:**

* The library is optimized for speed, making it suitable for real-time applications.
* Its performance is well-suited for both small-scale projects and large-scale systems.



## Conclusion

In conclusion, this project has realized a robust facial recognition-based identity verification system by seamlessly integrating pre-trained models, OpenCV, and the face\_recognition library. We've achieved a reliable mechanism for accurate identity confirmation in online assessments. The project's ethical considerations, coupled with its technological advancements, highlight its potential to contribute to secure online assessment platforms. This endeavor underscores the symbiotic relationship between innovation and ethics in shaping contemporary technological solutions.

The project's significance lies in its potential to significantly enhance the security and integrity of online assessment processes. Through the model's ability to swiftly and accurately match captured facial images against a database of preprocessed images, the system effectively addresses the challenge of impersonation and fraudulent activities during remote evaluations. This achievement aligns with the evolving landscape of educational technology, emphasizing the importance of trustworthy online assessment platforms.



## Application

**Secure Test-Taker Identity Verification:**

* Enhances the integrity of online assessments by accurately verifying the identity of test takers through facial recognition.
* Prevents impersonation and cheating during remote exams, ensuring fairness and credibility.

**Fraud Prevention in Online Assessments:**

* Detects and prevents impersonation attempts by cross-referencing test taker identities with a verified database.
* Enhances the reliability of assessment results and maintains the authenticity of educational outcomes.

**Customized Test Environment:**

* Recognizes authorized test takers and personalizes the test environment to their preferences.
* Creates a secure and tailored assessment experience for each individual.

**Reduced Administrative Burden:**

* Streamlines attendance tracking and verification processes, reducing administrative workload.
* Frees up resources for more valuable educational tasks.

**Enhanced Test Security and Integrity:**

* Augments the credibility of online assessments by employing advanced biometric identification.
* Safeguards the value of certifications and degrees by upholding the authenticity of test results.

**Future-Ready Educational Platforms:**

* Paves the way for the integration of facial recognition technology in educational systems of the future.
* Adapts to the evolving landscape of remote and digital learning.

A blue triangle with a red and white triangle

Description automatically generated

## System and Software Requirements

* Hardware: Standard computer with dual-core processor or higher, 4 GB RAM, webcam (720p resolution or higher).
* Software: Compatible with Windows 10, macOS 10.13+, Linux; web browsers: Chrome, Firefox, Edge.
* Network: Stable internet connection (1 Mbps or higher).
* Security: Secure HTTPS connection, firewall, antivirus; encrypted data transmission and storage.
* Device Mobility: Accessible on laptops, desktops, tablets.
* Environment: Well-lit, glare-free, quiet space for accurate facial recognition.

A blue triangle with a red and white triangle

Description automatically generated

## References

Educational Testing Service. (2021). **Using Facial Recognition for Remote Proctoring: Best Practices and Privacy Considerations**. Retrieved from

<https://www.ets.org/research/topics/remote-proctoring-facial-recognition>

Jones, M. (2022). **Facial Recognition in Online Assessments: Implementation Challenges and User Experience**. TechEd Insights Blog. Retrieved from

<https://techedinsights.com/facial-recognition-online-assessments>