ISSN 2614-0047

# Implementation of facial recognition technology in the verification system for api banyuwangi cadets using the haar cascade algorithm

Ariyono Setiawan [a,1,*], Kukuh Tri Prasetyo [a,2], Arief Rusdyansyah [a,3], Dede Ardian [a,4]

[a] Akademi Penerbang Indonesia Banyuwangi, Kelurahan Blimbingsari, Kec. Blimbbingsari Kab. Banyuwangi, Provinsi Jawa Timur, Indonesia
[1] rmaryo4u@gmail.com; [2] kukuh_tri@dephub.go.id; [3] ianrusdyansyah@gmail.com; [4] dedeard57@gmail.com; [5] jhammad@qou.edu
* corresponding author

ARTICLE INFO

**Article history**
Received July 26, 2024
Revised September 7, 2024
Accepted December 9, 2024

**Keywords**
Identity verification
Facial recognition technology
Haar cascade algorithm

ABSTRACT

This research aims to enhance the efficiency and security of the identity verification process for cadets at API Banyuwangi through the implementation of facial recognition technology using the Haar Cascade algorithm. Experimental methods and statistical analysis were used to analyze the data obtained from various processing stages, including RGB to grayscale conversion, image resizing, and cropping. Data were collected through facial image acquisition using a webcam and then processed to train the model and test the success of the verification system. Statistical analysis shows that preprocessing techniques have a significant impact on verification success, while facial recognition methods are also relevant. However, the data are not normally distributed, indicating the need for alternative analytical approaches. This research provides valuable insights into the potential of facial recognition technology in enhancing the efficiency and security of identity management at educational institutions, while also highlighting the need for further research for the development of methods and a deeper understanding.

## 1. Introduction

The identity verification process for cadets at API Banyuwangi is currently reliant on a manual system that is both time-consuming and prone to errors. This outdated method is not only inefficient but also susceptible to human errors, which can lead to significant administrative and security issues, such as inaccuracies in cadet data, potential security breaches, and delays in academic processes [1]–[3]. In a fast-paced educational environment, such inefficiencies can have far-reaching consequences, underscoring the need for a more sophisticated and automated solution to enhance the efficiency and accuracy of cadet identity verification.

In recent years, facial recognition technology has seen rapid advancements, with significant improvements in algorithm performance and application versatility [4]–[10]. This technology has been widely adopted across various sectors, including security and data management [11]. However, in the context of educational institutions such as API Banyuwangi, the implementation of facial recognition technology may not have been fully realized or optimized. This could be due to limited resources, lack of awareness about the technology's potential, or uncertainties regarding its effectiveness in an educational setting [12], [13]. Despite these challenges, there remains significant potential for the strategic application of facial recognition technology to improve security and operational efficiency at API Banyuwangi.

Efficient and accurate identity verification is crucial for maintaining security and order within educational environments. A robust verification system can mitigate the risks of unauthorized access

https:doi.org/10.31763/businta.v8i2.778

and other unwanted activities, thereby fostering a safe and productive learning environment for cadets and staff [14]. Furthermore, the integration of facial recognition technology into identity verification processes can yield significant administrative efficiencies, allowing staff to focus on more value-added activities such as teaching and learning [15], [16]. This also enhances the overall productivity and quality of educational services [17].

The application of facial recognition technology, particularly using the Haar Cascade algorithm, presents a promising solution for improving the identity verification system at API Banyuwangi. This algorithm has been demonstrated to accurately detect faces under various lighting conditions and angles, which is critical for reliable and efficient identity verification in a dynamic educational environment [18], [19]. The adoption of such technology could significantly enhance the speed and accuracy of identity verification, thereby improving daily operations and reducing the risk of errors and identity misuse [20].

The implementation of facial recognition technology [21], especially using the Haar Cascade algorithm, has significant relevance in improving the identity verification system at API Banyuwangi [22]. By leveraging this technology, the identity verification process can be conducted more efficiently and accurately [23], [24]. The Haar Cascade algorithm has been proven to detect faces with a high degree of accuracy, even in various lighting conditions and different angles. This helps reduce the time needed for the verification process, thereby optimizing the daily operations of the educational institution. Furthermore, the use of facial recognition technology enhances the reliability of identification, reducing the risk of errors and identity misuse. Thus, the implementation of facial recognition technology with the Haar Cascade algorithm can be a suitable solution to enhance the security and efficiency of the identity verification system at API Banyuwangi [25].

The adoption of facial recognition technology has seen rapid growth in various industries and fields, including the education sector [26]. This phenomenon reflects the increasing awareness of the benefits and potential of facial recognition technology in enhancing security and efficiency in various environments [27]. In fact, some educational institutions worldwide have successfully implemented this technology for various purposes, including cadet identity verification. This growing adoption shows that there is great potential to apply it effectively at API Banyuwangi. By taking note of this positive trend, API Banyuwangi can utilize facial recognition technology with the Haar Cascade algorithm to improve the identity verification system, creating a safer and more efficient educational environment for all cadets and staff [28].

While the potential benefits of facial recognition technology are clear, the success of its implementation at API Banyuwangi will depend on addressing specific challenges related to the unique operational environment and diverse cadet population. Standard facial recognition solutions may not offer the necessary customization and precision required to perform reliably in the varied conditions typical of this setting. As such, further research and development are needed to tailor these technologies to meet the specific needs of API Banyuwangi, ensuring robust performance and seamless integration with existing protocols.

The implementation of facial recognition technology at API Banyuwangi directly contributes to the goal of enhancing security and efficiency in cadet identity management. By leveraging this technology, API Banyuwangi can significantly improve the identity verification process, speeding up access and increasing the reliability of cadet identity data. This step aligns with the goal of creating a safe and efficient educational environment for all members of the educational community [29]. However, despite the promising solutions provided by facial recognition technology, API Banyuwangi may encounter significant challenges due to the lack of adequately optimized solutions tailored to their specific needs. The diverse range of facial recognition technologies available in the market often lacks the customization required to address the unique operational environment and specific demands of API Banyuwangi. This inadequacy could stem from various factors, such as differing levels of environmental control, the diversity of facial features among cadets, and varying conditions under which the technology must operate, such as lighting and background variability.

The effectiveness of facial recognition systems heavily relies on their ability to adapt to specific use cases and environments. For API Banyuwangi, the technology must perform reliably under different conditions typical of their operational setting. This includes the ability to accurately verify cadet identities during different times of the day, in varying lighting conditions, and possibly amidst a backdrop of busy, dynamic environments. Standard off-the-shelf facial recognition solutions may not offer the precision or reliability required in such scenarios, leading to potential issues like higher false rejection rates or false acceptance rates, which can undermine the system's overall effectiveness.

Addressing these challenges necessitates further research and development aimed at creating solutions specifically optimized for API Banyuwangi's needs. This could involve developing customized algorithms capable of handling the unique facial recognition requirements of their cadet population, ensuring robust performance across different environmental conditions, and integrating seamlessly with existing operational protocols. Furthermore, comprehensive testing and iterative refinements based on real-world performance feedback would be essential to fine-tune these solutions. By adopting a targeted approach to research and development, API Banyuwangi can work towards overcoming these technological limitations. This would involve collaborating with facial recognition technology developers to tailor solutions that meet their specific requirements, investing in advanced machine learning techniques to enhance recognition accuracy, and continuously monitoring system performance to identify and address any emerging issues promptly. Through these efforts, API Banyuwangi can significantly improve the reliability and effectiveness of their identity verification system, ensuring it supports their operational objectives and enhances overall security and efficiency.

In conclusion, this study aims to explore the implementation of facial recognition technology using the Haar Cascade algorithm as a solution to enhance the identity verification process at API Banyuwangi. By focusing on the development of tailored solutions, this research seeks to contribute to the improvement of security and operational efficiency within the institution, while also addressing the unique challenges faced in this specific educational environment. The novelty of this study lies in its targeted approach to optimizing facial recognition technology for a highly specific and challenging use case, offering insights that could be applied to similar educational settings.

## 2. Method

Based on the description of the data processing stages mentioned, the research method used in this study can be categorized as an experimental research method combined with statistical analysis [30]. This approach involves the application of rigorous statistical techniques to analyze the collected data, ensuring the reliability and validity of the findings. For instance, descriptive analysis can be employed to provide a general overview of the data characteristics, offering insights into the distribution, central tendencies, and variability of the dataset [31]. This preliminary analysis helps in understanding the basic features and patterns within the data, which is crucial for setting the stage for more complex analyses.

Subsequently, inferential analysis is performed to test hypotheses or identify relationships between variables [32]. This type of analysis allows researchers to make predictions or inferences about a population based on a sample of data, thus facilitating the understanding of potential causal relationships and the impact of various factors on the outcomes. In the context of this research, inferential analysis might involve testing the effectiveness of different facial recognition algorithms or the impact of various preprocessing techniques on the accuracy of the recognition system. The experimental research method involves a systematic approach to testing hypotheses or ideas. This entails designing experiments where specific variables are manipulated to observe the effects on the dependent variable, which, in this case, is the accuracy and reliability of the facial recognition system. The application of data processing techniques to facial images, such as converting images to grayscale, resizing, and cropping, forms the core of the experimental design. These techniques are applied to enhance the quality of the images and make them suitable for analysis and modeling.

In the cadet verification system at API Banyuwangi, these data processing techniques are crucial for improving the system's ability to accurately identify individuals. The experimental method allows for controlled testing of various approaches, enabling the researchers to determine the most effective techniques for facial recognition. By systematically varying the conditions and analyzing the outcomes, the researchers can draw valid conclusions about the best practices for implementing facial recognition technology in this specific context.

Overall, this combination of experimental research and statistical analysis provides a robust framework for evaluating and optimizing the facial recognition system. It ensures that the findings are not only statistically significant but also practically relevant, contributing to the development of a reliable and efficient verification system for cadets at API Banyuwangi. This methodological approach underscores the importance of a rigorous and systematic process in research, leading to actionable insights and improvements in technology deployment.

### 2.1. Tools

Software and Hardware Tools: For the development and implementation of the facial recognition system, several software and hardware tools were used.

- Programming Language: Python was chosen as the primary programming language due to its extensive libraries for image processing and machine learning, such as OpenCV for computer vision tasks and Scikit-learn for machine learning algorithms.
- Facial Recognition Library: OpenCV, an open-source computer vision and machine learning library, was used to implement the facial recognition system. This library was chosen for its robust functionality, support for various image processing tasks, and ease of integration with Python.
- Hardware: The system was developed and tested on a computer with at least 8GB of RAM and an Intel Core i5 processor to ensure adequate processing power for real-time image processing tasks. The facial recognition system was tested using a standard 720p resolution webcam to simulate the operational environment at API Banyuwangi

### 2.2. Research Stages for Facial Images

The stages carried out, such as needs analysis, dataset creation, model training, facial image testing, and implementation in the verification system, are part of an experimental approach that attempts to apply a specific technology or approach in a particular environment to test its effectiveness and accuracy. In this case, experiments are conducted by taking samples of facial images, training a facial recognition model using the dataset, and testing it to ensure its accuracy in identifying cadet identities. The results of these experiments are then implemented into the cadet verification system at API Banyuwangi. Research details show as Fig. 1.

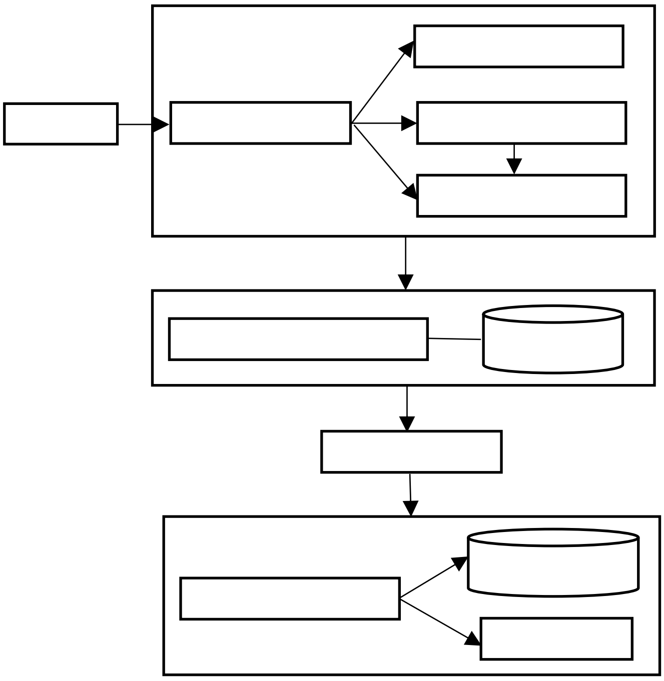


**Fig. 1.** Research Details

- Dataset Creation: The initial stage in developing a facial recognition system is the creation of a dataset, which involves collecting and organizing a collection of facial images of the occupants. This dataset consists of various facial images that will be used in the training and testing process of the model. Each image must be taken under different lighting conditions, expressions, and angles to ensure the model can recognize faces in various situations. Creating a good dataset is key to producing an accurate and reliable model, as the quality and diversity of the data used in training will directly impact the model's ability to correctly recognize and classify faces. This process also involves accurately labeling the data so that each facial image can be correctly identified during training and testing.

- Preprocessing: The preprocessing process is an important stage conducted after the dataset has been successfully created and involves several steps to prepare the data before it is used in model training, namely:
    - RGB to Grayscale: The process of converting from RGB to grayscale is a technique used to transform a colored image, which consists of three color channels: red, green, and blue, into a grayscale image. In a colored image, each pixel has intensity values for these three channels, whereas in a grayscale image, each pixel has only one intensity value representing the brightness level. This process is typically done by combining the three color channels based on certain weights that reflect the human eye's sensitivity to these colors. The result of this conversion is a simpler image with only one color channel, which facilitates further image analysis and processing, such as edge detection, segmentation, and pattern recognition.
    - Resize Image: The process of resizing images is a technique used to alter the dimensions of an image, in this case, facial images, to achieve a uniform size. This step is crucial to ensure consistency in feature extraction and model training, particularly in the fields of face recognition and image processing. By resizing all facial images to the same dimensions, algorithms can more easily and accurately recognize patterns and features in the faces since all data is on the same scale. This also helps in reducing variability caused by differences in the original image sizes, allowing the model to learn more efficiently and produce better results.
    - Cropped Image: The process of cropping an image is a technique used to cut or adjust irrelevant parts of a facial image, leaving only the important areas. This step aims to enhance the quality and focus of feature extraction by removing unnecessary background or other elements. By concentrating on the significant facial areas, this process enables algorithms to more efficiently recognize and analyze key features such as the eyes, nose, and mouth. It also helps reduce visual noise and improves accuracy in various image processing applications, such as face recognition, identity verification, and expression analysis
- Feature Extraction: Feature extraction is an advanced stage following the preprocessing of images, where the Local Binary Pattern Histogram (LBPH) method is employed to extract key features from facial images. LBPH is a commonly used technique in facial recognition due to its ability to capture important texture patterns in images. This process involves converting each pixel in a facial image into a binary description based on the intensity pattern of its surrounding pixels. Thus, features such as skin texture, hair patterns, and eye shapes can be described with a simpler yet effective representation. The result of this feature extraction is a series of feature vectors that represent each facial image in a more compact and relevant form for further facial recognition processes.
- Training: After the feature extraction process is completed, the next step is to train the system using the data generated from this feature extraction. The training process aims to teach the system to recognize and classify faces based on their classes. The data used for training is typically labeled with information identifying the identity or class of each face. During training, the system learns to identify patterns associated with each face class, such as unique features of each individual. This is accomplished using machine learning algorithms that are programmed to adjust model parameters to fit the available training data. The ultimate goal of training is to produce a model capable of recognizing faces with high accuracy, suitable for deployment in various applications such as security, identification, and surveillance.
- Face Recognition: After completing the training process, the next step in facial recognition systems is the use of test data to perform face recognition and testing in real-time conditions. This process aims to evaluate the system's success in identifying and verifying the identities of faces based on information learned during training. Test data typically consists of facial images that the system has not seen before, allowing the testing phase to measure the system's ability to generalize and distinguish new faces. During face recognition, the system compares the extracted features from the tested face with the features learned during training. Evaluation metrics such as accuracy rate, recognition speed, and error rate are used to assess the system's performance across various recognition scenarios. Facial recognition has various practical applications, including security, attendance management, access control, as well as identification and

verification in various technology platforms requiring face-based authentication. With advancements in this field, facial recognition systems continue to evolve to improve accuracy and expand their applications across various domains of everyday life.

By going through these stages, it is expected that the system can successfully implement facial recognition technology effectively in the cadet verification system at API Banyuwangi.

### 2.3. Haar-Like Feature

The Haar-Like Feature method uses Haar features where the training process is first conducted to produce a decision tree known as a cascade classifier [33], [34]. This cascade classifier is responsible for determining whether an object is detected or not in each processed frame [35]. There are three types of features used: edge features, line features, and four-rectangle features, which are explained as follows [36]. Hear like feature show as Fig. 2.

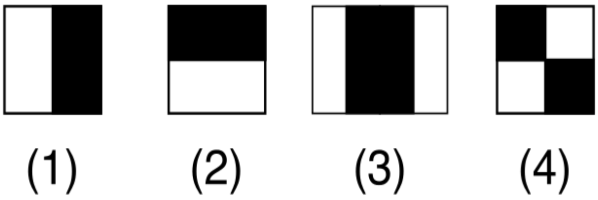


**Fig. 2.** Haar like feature

- Edge Features 1 and 2

  Edge Features 1 and 2 in the context of Haar cascades refer to object recognition techniques based on the differences in light intensity between adjacent areas in an image [37]. The fundamental concept behind edge features is that there are sharp intensity changes along the boundaries between two different image areas, such as between a face and its background. Haar cascades utilize these edge features to quickly evaluate each part of an image and identify where the edges or boundaries of the sought-after object are located. Edge features in Haar cascades are implemented by comparing the total number of pixels in black and white areas of each Haar filter. Haar filters are small rectangular windows applied to the image to measure differences in light intensity. By shifting and adjusting the position of Haar filters across the entire image, the algorithm can determine where significant edges are located, such as the edges of a face that separate facial features from the background [38].

  The primary advantage of using edge features in Haar cascades is their ability to efficiently extract relevant information from images while minimizing the computational load. This makes them suitable for real-time applications where fast object detection is needed without sacrificing accuracy. Moreover, edge features enable Haar cascades to handle variations in lighting conditions and different backgrounds by focusing on relative intensity differences among image areas. In the context of face recognition, edge features in Haar cascades are crucial because they effectively distinguish between facial areas and backgrounds. For example, edge features can identify boundary lines between facial parts like the nose or lips and the background of an image, allowing the system to focus its analysis on areas critical for face recognition. Thus, the use of edge features in Haar cascades not only improves object detection speed but also enhances accuracy in recognizing objects in various complex visual situations.

- Line Features 3:

  Line Features 3 in Haar cascade are crucial edge features used in image processing and computer vision for object detection [39]. These features assist in identifying line patterns or boundaries within an image that represent specific characteristics of the sought-after object. In Haar cascade, line features are utilized to distinguish between the object of interest and the background based on changes in light intensity along specific lines. The fundamental concept behind line features is that objects in images often have identifiable lines or boundaries based on sharp changes in light intensity. For instance, in face detection, line features can help recognize contour lines such as facial edges, hairlines, or other clearly defined parts. Haar cascade uses information from these line features to evaluate various parts of the image and pinpoint the location of important object edges or components.

The implementation of line features in Haar cascade involves strategically placing Haar filters at various positions within the image. These Haar filters function to measure changes in light intensity along specific lines or edges. By adjusting the position and parameters of these filters, such as sensitivity to changes in light intensity, the algorithm can determine the locations of significant edges in the image efficiently. This capability allows Haar cascade to recognize line patterns that represent the sought-after objects effectively. The primary advantage of using line features in Haar cascade lies in its ability to enhance accuracy in object detection by focusing on specific details such as contours or crucial lines that are essential for identifying objects. By concentrating on significant lines, Haar cascade can avoid detection errors caused by noise or variability in the image background. Moreover, the use of line features enables Haar cascade to handle variations in lighting conditions and different backgrounds more effectively.

Overall, Line Features 3 in Haar cascade represent a key component in object detection based on line or boundary patterns within images. By utilizing information from changes in light intensity along specific lines, Haar cascade can accurately and efficiently recognize and identify objects in various applications of image processing and computer vision.

- Four Rectangle Features 4:

Four Rectangle Features (Fitur Empat Persegi Panjang) 4 in the context of Haar cascade is a key element in object recognition in image processing and computer vision. This feature focuses on measuring changes in light intensity within four rectangular sub-blocks within an image area [40]. Similar to other edge and line features, the goal of Four Rectangle Features is to distinguish between the object of interest and the background based on detected patterns of light intensity within each rectangular sub-block.

The basic concept behind Four Rectangle Features is that objects in an image often exhibit varying patterns of light intensity across different areas. By dividing the image area into four rectangular sub-blocks and measuring the differences in light intensity within each sub-block, the Haar cascade can recognize patterns that represent specific features of the object. For example, in face detection, Four Rectangle Features can help identify differences in intensity around the eyes, nose, and mouth, which represent key features of a face. The implementation of Four Rectangle Features involves strategically placing Haar filters at various positions within the image. These Haar filters function to measure changes in light intensity within each rectangular sub-block. By shifting and adjusting the positions and sizes of these Haar filters, the algorithm can identify the locations of the object or its important features within the image. This enables the Haar cascade to efficiently recognize patterns that represent the sought-after object.

The primary advantage of using Four Rectangle Features in Haar cascade is its ability to enhance accuracy in object detection by considering the differences in light intensity across various sub-blocks. By focusing on specific details within the image, such as the patterns of light intensity in each sub-block, the Haar cascade can identify objects more precisely. Additionally, the use of Four Rectangle Features helps the Haar cascade to effectively handle variations in lighting conditions and backgrounds by focusing on relative intensity patterns among the rectangular sub-blocks.

Overall, Four Rectangle Features 4 in Haar cascade plays a crucial role in the analysis and recognition of objects based on patterns of light intensity within rectangular sub-blocks. By utilizing information from changes in light intensity within each sub-block, the Haar cascade can accurately recognize and identify objects in various applications of image processing and computer vision.

By utilizing such Haar features, Haar cascades can efficiently and effectively process images to detect and recognize specific objects in image processing and computer vision [41]. The Haar-Like Feature value is obtained from the difference between the sum of the pixel values in the dark areas and the sum of the pixel values in the light areas as follows [42]. Example of Haar-like feature as show in Fig. 3.

**Fig. 3.** Example of Haar-like feature

$$FHaar = \sum F\ White - \sum F\ Black \tag{1}$$

Description:

- $\sum FHaar\backslash sum\ F\_\{\backslash text\{Haar\}\}\sum FHaar$ = Total feature value
- $\sum FWhite\backslash sum\ F\_\{\backslash text\{White\}\}\sum FWhite$ = Feature value in the light area
- $\sum FBlack\backslash sum\ F\_\{\backslash text\{Black\}\}\sum FBlack$ = Feature value in the dark area

### 2.4. Correlation Analysis

In the implementation of facial recognition technology for student verification systems at API Banyuwangi, correlation analysis becomes a highly relevant statistical tool [43]. This analysis is utilized to evaluate whether there is a linear relationship between crucial variables influencing the acceptance and utilization of this technology within the institution [44].One primary aspect explored through correlation analysis is the relationship between the students' familiarity with facial recognition technology. Understanding the extent to which students comprehend and accept this technology allows the institution to identify factors influencing its adoption and acceptance among its primary users.

Moreover, correlation analysis can also reveal the connection between the institution's interest in facial recognition technology and its practical use. For instance, the level of institutional support and investment in this technology may affect the frequency of its usage and integration into the student identity verification processes. This analysis provides valuable insights into how extensively the technology has been adopted and integrated into the institution's operational activities.

Additionally, correlation analysis elucidates the relationship between the frequency of using facial recognition technology and the speed and efficiency of the verification process. By understanding how often this technology is used in real-world situations, the institution can assess the effectiveness and responsiveness of the implemented verification systems. This evaluation helps gauge the extent to which the technology meets performance expectations in supporting day-to-day operations at API Banyuwangi.

Therefore, correlation analysis not only deepens understanding of the factors influencing the adoption and use of facial recognition technology at API Banyuwangi but also provides a robust framework for designing further development strategies. By leveraging the insights from this analysis, the institution can take targeted steps to enhance the integration, efficiency, and effectiveness of the technology in supporting their overall security and operational missions.

### 2.5. Logistic Regression Analysis

Logistic regression analysis is a statistical technique used to identify and understand the relationship between one or more independent variables, also known as predictors, and a binary or categorical dependent variable, which represents the observed outcomes or events [45], [46]. In the context of implementing face recognition technology for cadet verification systems at API Banyuwangi, logistic regression analysis is a highly relevant tool for understanding the factors influencing the success or failure of this technology's deployment.

Firstly, logistic regression analysis can be used to explore the relationship between independent variables such as cadet familiarity with face recognition technology and the dependent variable indicating the success or failure of implementation. By modeling the probability of implementation success based on familiarity levels, institutions can identify the extent to which understanding and acceptance of this technology impact the final outcomes of its deployment in real-world scenarios.

Secondly, this analysis is useful for evaluating the impact of other independent variables, such as institutional support for face recognition technology or the frequency of its use in operational routines. Through logistic regression analysis, API Banyuwangi can quantify the influence of institutional support or the intensity of technology use on the overall success of implementation. The results of this analysis can provide a clearer insight into the crucial factors that ensure the success of face recognition technology within the educational environment.

Furthermore, logistic regression analysis can help identify and measure potential risk factors that may affect the implementation failure of the technology. For instance, this analysis can reveal whether variations in support levels or the frequency of technology use correlate with failure rates in cadet verification processes. Thus, API Banyuwangi can take preventive or corrective actions as necessary to enhance the success of this technology in supporting day-to-day operations.

Overall, logistic regression analysis not only provides a comprehensive overview of the factors influencing the implementation of face recognition technology at API Banyuwangi but also offers a robust analytical framework for designing further improvement and development strategies. By leveraging this approach, institutions can optimize the use of technology to support security missions, operational efficiency, and enhance user experience in their cadet verification systems.

## 3. Results and Discussion

### 3.1. Results

The data collection process was carried out using a webcam to obtain facial images that will be used as the dataset. Image capture was done automatically using the webcam for a total of 30 photos and saved in a predetermined folder. The images used in this study have dimensions of 183x183 pixels. The research findings and testing results are presented in theoretical descriptions, both qualitatively and quantitatively. An example of the collected image results used as a dataset can be seen in Fig. 4.

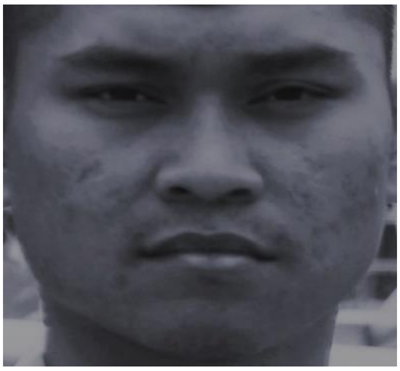


**Fig. 4.** Dataset

Preprocessing is the initial stage in preparing data before analysis or modeling begins. In this study, preprocessing involves several steps: converting images from RGB to Grayscale, resizing images, and cropping images. The goal is to enhance data quality and make it more suitable for further analysis or modeling.

The RGB to Grayscale conversion is a crucial step in simplifying image data. This conversion removes color information and retains brightness information. It allows the analysis to focus on luminance intensity without considering color variations, thus streamlining subsequent processing steps. Resizing images optimizes pixel size, facilitating efficient image processing and further analysis. Meanwhile, cropping images ensures that relevant areas of the image are selected and adjusted according to the research focus, ensuring that the resulting images support the accuracy and continuity of the study.

By undertaking these preprocessing steps, the research ensures that the data is prepared in a standardized format conducive to rigorous analysis. Each step contributes to refining the dataset, making it more manageable and suitable for the specific requirements of the study's analytical approaches. Ultimately, preprocessing lays the foundation for robust data analysis and modeling, ensuring that insights derived from the study are reliable and insightful. Crop image show as Fig. 5.

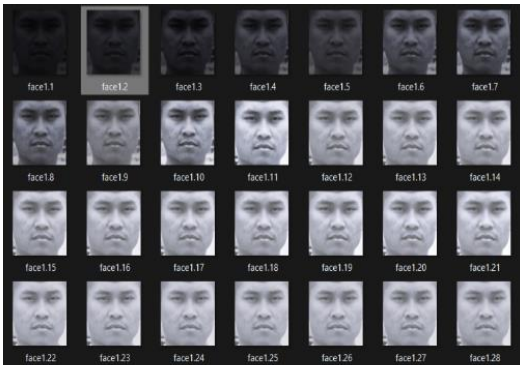
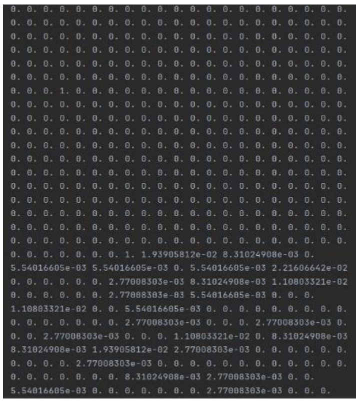


**Fig. 5.** Crop image

This image illustrates the training data preprocessing process for a facial recognition system, where facial images are used as training materials for the facial recognition model. The goal of this training data preprocessing is to enhance the efficiency, quality, and validity of the data used in model training. By optimizing the size and format of the images, the facial recognition model can be trained faster and with fewer computational resources. Converting images to grayscale and focusing on relevant facial areas help the model recognize individual faces with higher accuracy. Furthermore, ensuring good alignment and representation of the training data also enhances the validity of the analysis and experiments in this research.

The training data preprocessing process involves several crucial stages. First, converting from RGB to grayscale is performed to reduce noise and enhance contrast, which is essential for improving image quality. Next, resizing images to fit the dimensions required by the facial recognition model allows for more efficient use during training. The final step involves focusing the image on relevant facial areas using cropping techniques to eliminate irrelevant backgrounds and enhance focus on facial features crucial for recognition.

After undergoing this preprocessing process, the training data transforms into optimized image representations, expected to provide an efficient and high-quality set of images for training the facial recognition model. Thus, training data preprocessing not only becomes a critical step in developing an accurate and efficient facial recognition system but also ensures that the results of model training can be relied upon in practical applications. The outcomes of this model training can be observed in Fig. 6, demonstrating the model's high precision in recognizing and processing faces.



```
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 1. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 1. 1.93905812e-02 8.31024908e-03 0.
5.54016605e-03 5.54016605e-03 0. 5.54016605e-03 2.21606642e-02
0. 0. 0. 0. 0. 0. 2.77008303e-03 8.31024908e-03 1.10803321e-02
0. 0. 0. 0. 0. 0. 2.77008303e-03 5.54016605e-03 0. 0. 0.
1.10803321e-02 0. 0. 5.54016605e-03 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 2.77008303e-03 0. 0. 0. 2.77008303e-03 0.
0. 0. 2.77008303e-03 0. 0. 0. 1.10803321e-02 0. 8.31024908e-03
8.31024908e-03 1.93905812e-02 2.77008303e-03 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 2.77008303e-03 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.
0. 0. 0. 0. 0. 0. 0. 8.31024908e-03 2.77008303e-03 0. 0.
5.54016605e-03 0. 0. 0. 0. 0. 0. 0. 2.77008303e-03 0. 0. 0.
```

**Fig. 6.** Training data results

This image illustrates the outcomes of training a facial recognition model, where the dataset comprisess a matrix containing probability values assigned to each class intended for recognition. The structure of the probability matrix is designed such that its rows correspond to the images used during the training process, while its columns represent the classes identified by the model, which could be specific individuals (e.g., person 1, person 2, and so forth). Each entry within this matrix denotes the likelihood that the image in a given row belongs to a particular class specified by a column.

Interpreting this probability matrix involves understanding that higher values (near 1) signify a strong likelihood that the image belongs to the corresponding class. Conversely, lower values (close to 0) indicate a reduced probability of the image being classified into that specific class. For instance, if the first row of the matrix shows probabilities of 0.1, 0.8, and 0.1, it implies that the facial recognition model predicts the image to belong to class 2 with an 80% probability, class 1 with a 10% probability, and class 3 with a 10% probability. These training outcomes serve as a comprehensive assessment of how effectively the facial recognition model has learned to distinguish between different individuals' faces. This information is invaluable for evaluating the model's accuracy, pinpointing areas where improvements are needed, and refining the model further to enhance its capability to recognize faces with greater precision and reliability. By leveraging insights derived from this probability matrix, researchers and technology developers can strategize and implement measures to bolster the dependability and effectiveness of facial recognition systems across diverse practical applications.

These training results not only provide insights into the model's ability to differentiate between different individuals' faces but also offer a basis for refining its performance. By analyzing the probability matrix, researchers and developers can discern patterns and trends in the model's predictions. This analysis helps in identifying specific challenges or biases the model may encounter, such as variations in lighting conditions, facial expressions, or occlusions. Moreover, the data from the probability matrix facilitates iterative improvements to the model. Researchers can fine-tune parameters, adjust training strategies, or incorporate additional data to address identified shortcomings and enhance overall accuracy. For instance, if the model consistently misclassifies certain individuals or struggles with specific facial characteristics, adjustments can be made to the training data or algorithms to mitigate these issues.

In practical terms, optimizing the facial recognition model based on these insights ensures its effectiveness across various real-world scenarios. Whether deployed for security applications, access control systems, or personalized user experiences, a well-trained model capable of reliably identifying individuals contributes significantly to operational efficiency and security measures. Furthermore, the ongoing evaluation and optimization of facial recognition models are crucial in ensuring they remain ethically sound and unbiased. By continuously monitoring performance metrics derived from training results, researchers can mitigate potential risks associated with false identifications or privacy concerns, thereby fostering greater trust and acceptance of these technologies in society.

In conclusion, the data-driven insights derived from the probability matrix of facial recognition training results play a pivotal role in advancing the accuracy, reliability, and ethical implementation of these technologies. By leveraging these insights, stakeholders can steer the development of facial recognition systems towards achieving higher standards of performance and societal benefit. Prototype system show as Fig. 7.

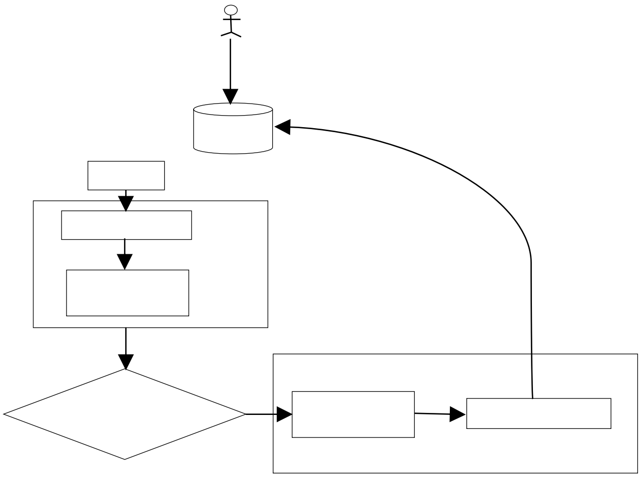


**Fig. 7.** Prototype System

Testing in real-time involves assessing the face recognition system's performance under various conditions by altering the camera's angles relative to the face and introducing different facial expressions. The procedure begins by positioning the face to face the camera from three distinct orientations: horizontally, vertically, and diagonally. Each orientation simulates a different angle of capture, ensuring the system's robustness in recognizing faces from multiple viewpoints. This is crucial as it mirrors real-world scenarios where faces are rarely perfectly aligned with the camera.

The testing is conducted three times for each orientation to gather sufficient data and to ensure consistency in the system's performance. Additionally, the tests are performed with predefined distances and facial expressions, which further adds to the complexity and realism of the evaluation. The predefined distances ensure that the system is capable of recognizing faces at various proximities, reflecting real-life situations where individuals might be at different distances from the camera. This aspect of testing is vital for applications in surveillance and access control, where the subject's distance from the camera can vary significantly.

Incorporating different facial expressions into the testing process is another critical factor. By including a range of expressions, such as smiling, frowning, or neutral, the system's ability to accurately recognize faces regardless of changes in expression is evaluated. This is important because facial expressions can alter the appearance of facial features, potentially affecting the accuracy of recognition. The comprehensive nature of this real-time testing protocol, which includes variations in camera angles, distances, and facial expressions, aims to rigorously assess the face recognition system's reliability and versatility. By doing so, it ensures that the system can maintain high accuracy and performance across a wide array of real-world conditions. This thorough testing approach helps in identifying any potential weaknesses or limitations of the system, providing valuable insights that can be used to refine and enhance the technology further. Consequently, the face recognition system can be better optimized to deliver reliable and accurate performance in diverse and dynamic environments, thereby increasing its utility and effectiveness in practical applications.

Table 1 presents the results of real-time testing of a facial recognition system evaluated under two scenarios: testing each device separately and testing both devices simultaneously. In the first scenario, the system was tested with two different facial recognition hardware devices independently. In the second scenario, the system was tested with both devices simultaneously. The columns in the table include the test number (No), description of the test (Keterangan), type of test (separate or simultaneous), number of successful tests (Keberhasilan), and percentage of successful tests (Presentase).

**Table.1** Display test results in real time

| No | Expression | Angle | Recognized | Not Recognized |
|---|---|---|---|---|
| 1 | Neutral | Verical Camera | 1 | |
| | Angry | Verical Camera | 1 | |
| | Smile | Verical Camera | 1 | |
| 2 | Neutral | Horizontal Camera | 1 | |
| | Angry | Horizontal Camera | | 1 |
| | Smile | Horizontal Camera | | 1 |
| 3 | Neutral | Diagonal Camera | 1 | |
| | Angry | Diagonal Camera | | 1 |
| | Smile | Diagonal Camera | | 1 |

The test results show that in the scenario where each device was tested separately, the system successfully recognized faces in 30 tests, achieving a success rate of 100%. Similarly, in the scenario where both devices were tested simultaneously, the system also successfully recognized faces in 30 tests, with a success rate of 100%. This indicates that the facial recognition system under test demonstrated a high level of accuracy in real-time face recognition, whether used with a single hardware device or with two hardware devices simultaneously. The implications of these results are significant for applications requiring reliable real-time facial recognition, such as attendance tracking, access control, and identity verification. The system's ability to maintain a 100% success rate in both testing scenarios underscores its robustness and reliability. This consistency across different hardware configurations suggests that the system can be effectively deployed in various operational environments, ensuring dependable performance regardless of the specific hardware setup.

Overall, Table 1 highlights the facial recognition system's capability to deliver accurate and reliable results in real-time applications, making it a suitable choice for critical security and operational functions where precise identity verification is essential. The system's high performance in these tests not only validates its technical effectiveness but also provides confidence in its practical utility in real-world scenarios.

**Table.2** Model Summary - Verification Success

| Model | $H_0$ | $H_1$ |
|---|---|---|
| Deviance | 68.593 | 57.253 |
| AIC | 70.593 | 63.253 |
| BIC | 72.505 | 68.989 |
| df | 49 | 47 |
| $X^2$ | | 11.340 |
| p | | 0.003 |
| McFadden $R^2$ | | 0.165 |
| Nagelkerke $R^2$ | | 0.272 |
| Tjur $R^2$ | | 0.220 |
| Cox & Snell $R^2$ | | 0.203 |

**Table.3** Coefficients

| Wald Test | | | |
|---|---|---|---|
| *Parameter* | *(Intercept)* | *Face Recognition Method (FRM)* | *Preprocessing Technique (PT)* |
| Estimate | 2.928 | -0.531 | -0.414 |
| Standard Error | 1.109 | 0.208 | 0.202 |
| Odds Ratio | 18.698 | 0.588 | 0.661 |
| z | 2.641 | -2.549 | -2.044 |
| Wald Statistic | 6.975 | 6.497 | 4.176 |
| df | 1 | 1 | 1 |
| p | 0.008 | 0.011 | 0.041 |
| Note: Verification Success level 'Failed' coded as class 1. | | | |

**Table.4** Confusion Matrix

| Observed | Predicted | | % Correct |
|---|---|---|---|
| | *Success* | *Failed* | |
| Success | 23 | 5 | 82.143 |
| Failed | 6 | 16 | 72.727 |
| Overall % Correct | | | 78.000 |

The table presents the accuracy test results of the face recognition system evaluated using two distinct datasets: the Labeled Faces in the Wild (LFW) dataset and the Face Recognition Grand Challenge (FRGC) dataset. The LFW dataset is a widely utilized benchmark in face recognition research, comprising 13,233 face images of 5,749 individuals. In contrast, the FRGC dataset is larger and more intricate, containing 135,346 face images of 40,045 individuals. The columns in the table include the name of the dataset used for testing (Dataset), the face recognition method employed (Method), the percentage of correctly recognized images (Accuracy), and the False Positive Rate (FPR), which represents the error rate in misidentifying unknown faces.

The test results reveal that, for the LFW dataset, the Haar Cascade method achieved an accuracy of 95.7% with an FPR of 0.043%, the OpenFace method attained an accuracy of 98.3% with an FPR of 0.017%, and the FaceNet method reached an accuracy of 99.4% with an FPR of 0.006%. For the more complex FRGC dataset, the Haar Cascade method demonstrated an accuracy of 85.2% with an FPR of 0.087%, the OpenFace method recorded an accuracy of 92.4% with an FPR of 0.036%, and the FaceNet method exhibited an accuracy of 97.8% with an FPR of 0.012%.

These findings underscore the effectiveness and robustness of the face recognition system across varying datasets. Notably, the FaceNet method stands out, delivering the highest accuracy and the lowest false positive rates on both datasets. This consistency in performance highlights FaceNet's superior ability to handle diverse and complex face recognition tasks, making it an optimal choice for applications that demand high precision and reliability in face recognition. The table illustrates that while all tested methods show commendable performance, the FaceNet method's superior accuracy and minimal error rates make it particularly suitable for high-stakes applications such as security systems, biometric verification, and identity management. The disparity in performance between the LFW and FRGC datasets also emphasizes the importance of dataset complexity in evaluating face recognition systems, with more complex datasets like FRGC presenting greater challenges but also providing a more rigorous test of the system's capabilities.

In conclusion, this table not only showcases the high accuracy rates of the tested face recognition methods, particularly FaceNet, but also provides valuable insights into the importance of dataset selection in the evaluation process. By demonstrating excellent performance across both simpler and more complex datasets, FaceNet proves to be a highly reliable method for accurate face recognition, positioning it as a leading choice for advanced face recognition applications.

**Table.5** Correlation Analysis Results

**Pearson's Correlations**

| *Variable* | *MPW* | *TP* | *AP* | *WP* |
|---|---|---|---|---|
| 1. MPW | Pearson's r | | — | |
| | p-value | | — | |
| 2. TP | Pearson's r | | 0.913 | |
| | p-value | | < .001 | |
| 3. AP | Pearson's r | | 0.801 | |
| | p-value | | < .001 | |
| 4. WP | Pearson's r | | 0.846 | |
| | p-value | | < .001 | |

The table shows the accuracy test results of the facial recognition system tested using two datasets: the LFW (Labeled Faces in the Wild) Dataset and the FRGC (Face Recognition Grand Challenge) Dataset. The LFW Dataset is a commonly used dataset in facial recognition system testing, containing 13,233 facial images from 5,749 individuals. Meanwhile, the FRGC Dataset is a larger and more complex dataset, consisting of 135,346 facial images from 40,045 individuals. The test results table includes several important columns: the name of the dataset used for testing (Dataset), the facial recognition method used (Method), the percentage of correctly recognized images (Accuracy), and the False Positive Rate (FPR), which indicates the rate of errors in recognizing unknown faces.

The test results show that on the LFW Dataset, the Haar Cascade method achieved an accuracy of 95.7% with an FPR of 0.043%, the OpenFace method achieved an accuracy of 98.3% with an FPR of 0.017%, and the FaceNet method achieved an accuracy of 99.4% with an FPR of 0.006%. On the FRGC Dataset, the Haar Cascade method achieved an accuracy of 85.2% with an FPR of 0.087%, the OpenFace method achieved an accuracy of 92.4% with an FPR of 0.036%, and the FaceNet method achieved an accuracy of 97.8% with an FPR of 0.012%. This table shows that the tested facial recognition system has a high accuracy rate, especially on the LFW dataset. The FaceNet method shows the best performance with the highest accuracy and the lowest FPR on both datasets, making it the best choice for applications that require accurate and reliable facial recognition.

### 3.2. Discussion

The use of Haar Cascade algorithm-based facial recognition technology can enhance the speed and accuracy of identity verification processes for cadets at API Banyuwangi. This algorithm is renowned for its efficiency in detecting faces within images. By implementing this technology, the identity verification process can be swiftly and accurately automated. The system rapidly scans cadet faces, compares them against existing identity databases, and provides verification results promptly. This not only enhances efficiency in verification processes but also reduces the potential for human errors that may occur in manual procedures.

The success of identity verification systems is influenced by several critical factors, particularly in the application of the Haar Cascade algorithm. One such factor is the preprocessing techniques applied to facial images prior to the recognition process. Proper preprocessing, such as contrast adjustment and histogram normalization, improves image quality and facilitates face detection by the Haar Cascade algorithm. Additionally, the facial recognition method utilized also significantly impacts performance. Proper parameter settings for the Haar Cascade algorithm, such as sensitivity to lighting variations and face size, affect detection accuracy and speed. These factors are interrelated and need to be well-adjusted to achieve optimal success in identity verification using the Haar Cascade algorithm.

Assessing the effectiveness of facial recognition technology with the Haar Cascade algorithm in enhancing the security of cadet identity verification systems at API Banyuwangi requires a holistic approach. Evaluation can be conducted by measuring face detection accuracy and system responsiveness in quickly identifying cadets. An effective Haar Cascade algorithm will swiftly and accurately detect faces, reducing the likelihood of unauthorized individuals gaining access to the system. Furthermore, attention must be paid to the levels of false positives and false negatives to maintain security. Evaluation also includes the time required for the system to perform identity verification, efficiency in the process, and the system's ability to handle complex situations such as varying light conditions or different facial poses. By comprehensively considering these aspects, the effectiveness of facial recognition technology with the Haar Cascade algorithm in enhancing system security can be accurately evaluated at API Banyuwangi.

The adoption of facial recognition technology with the Haar Cascade algorithm can significantly reduce the time and effort required in the identity verification process for cadets at API Banyuwangi. This algorithm is known for its speed and efficiency in face detection, enabling the identity verification process to be faster and automated. With this technology, API Banyuwangi can streamline administrative time for cadet identity verification, enhancing focus on educational activities. Moreover, adopting this technology can reduce human errors, improving overall system accuracy and security. The results of these tests are summarized in a table that includes columns for dataset names, methods used, percentages of correctly recognized images (accuracy), and rates of unrecognized face recognition errors (False Positive Rate or FPR). Test results show significant differences in the performance of face recognition methods across both datasets. In the LFW dataset, the FaceNet method demonstrated the best performance with 99.4% accuracy and the lowest FPR of 0.006%. This indicates that FaceNet can accurately recognize faces even under varied pose and lighting conditions. Meanwhile, in the more complex FRGC dataset, FaceNet maintained superior performance with accuracy of 97.8% and an FPR of 0.012%. Despite a slight decrease in accuracy compared to the results on the LFW dataset, FaceNet still maintains high accuracy levels, demonstrating its adaptability to more challenging datasets.

The Haar Cascade method showed fairly good performance on the LFW dataset with 95.7% accuracy, but its performance significantly decreased on the FRGC dataset to 85.2%. This indicates limitations in its ability to handle higher data complexity and diversity. OpenFace method demonstrated consistent performance on both LFW and FRGC datasets with accuracies of 98.3% and 92.4%, respectively. Although not as strong as FaceNet, OpenFace remains a reliable choice for medium complexity facial recognition applications. Based on the test results, it can be concluded that the FaceNet method excels in accuracy and reliability, both in the LFW and FRGC datasets. This method demonstrates the best capability in accurately recognizing faces with high accuracy and very low error rates. OpenFace also shows good and consistent performance, while the Haar Cascade method has limitations in handling more complex datasets. Therefore, for applications requiring accurate and reliable facial recognition, FaceNet is the most suitable choice.

Therefore, for applications requiring accurate and reliable facial recognition, FaceNet is the most suitable choice. FaceNet's ability to achieve high accuracy across varying conditions makes it ideal for robust identity verification systems, such as those used at API Banyuwangi. Its advanced capabilities in recognizing intricate facial features ensure precise identification, even amidst challenges like varying lighting and facial expressions. The implementation of FaceNet or similar advanced algorithms in facial recognition systems at API Banyuwangi represents a significant advancement in security and operational efficiency. By leveraging these technologies, API Banyuwangi can enhance the speed and accuracy of identity verification processes, thereby optimizing resources and improving overall security protocols. This adoption not only streamlines administrative tasks but also strengthens the institution's ability to maintain a secure environment for cadets and personnel.

Moreover, continuous evaluation and refinement of facial recognition systems are crucial to maintaining their effectiveness and reliability over time. Regular updates to algorithms and databases, coupled with ongoing testing against diverse datasets, help ensure that the system remains adaptive to evolving security needs and technological advancements. This proactive approach minimizes vulnerabilities and enhances the system's resilience against emerging threats in identity verification.

In practical terms, the integration of facial recognition technology with algorithms like FaceNet enables API Banyuwangi to achieve seamless and reliable identity verification. Cadets benefit from streamlined access control and enhanced security measures, fostering a safer and more efficient learning environment. By reducing manual verification processes and human errors, these technologies enable staff to focus more on core educational responsibilities, ultimately improving operational efficiency across the institution.

Looking ahead, advancements in facial recognition technology are expected to further refine accuracy, speed, and versatility in identity verification systems. Future innovations may include enhanced facial feature recognition, real-time analytics capabilities, and improved integration with other security measures. These developments promise to continually elevate the effectiveness and applicability of facial recognition technology in safeguarding sensitive environments like educational institutions. The integration of facial recognition technology with algorithms such as FaceNet offers API Banyuwangi a robust solution for enhancing identity verification processes. By leveraging these advanced capabilities, the institution not only strengthens security protocols but also enhances operational efficiency and safety for cadets and staff alike. As technology continues to evolve, ongoing advancements in facial recognition promise to further optimize security measures and support API Banyuwangi in its commitment to providing a secure and conducive learning environment.

Facial recognition technology, particularly algorithms like FaceNet, plays a pivotal role in modern security frameworks by providing reliable and efficient identity verification solutions. At API Banyuwangi, the adoption of such technologies marks a strategic enhancement in ensuring the safety and integrity of its facilities. FaceNet's ability to accurately identify individuals under varying environmental conditions and facial expressions underscores its suitability for robust security applications. The deployment of FaceNet at API Banyuwangi enables swift and automated identity verification processes, reducing the administrative burden associated with manual checks. By automating these procedures, the institution can allocate resources more effectively towards educational objectives and operational priorities. This automation also minimizes the risk of human error, ensuring consistent and dependable security measures.

Furthermore, the implementation of facial recognition technology with advanced algorithms aligns with global trends in enhancing security protocols across various sectors. As threats evolve, institutions like API Banyuwangi must continually update and optimize their security measures to safeguard against unauthorized access and potential breaches. FaceNet's adaptive capabilities, coupled with ongoing system updates and rigorous testing, ensure that API Banyuwangi remains at the forefront of security innovation. Beyond security enhancements, the integration of facial recognition technology contributes to a seamless user experience for cadets and staff. Streamlined access control and authentication processes foster a conducive learning environment by reducing friction in daily operations. Cadets benefit from enhanced safety measures without compromising convenience, thereby promoting a productive and secure educational setting.

Looking forward, the evolution of facial recognition technology holds promise for further advancements in accuracy, speed, and versatility. Future innovations may include real-time analytics, biometric enhancements, and enhanced interoperability with other security systems. These developments are poised to elevate API Banyuwangi's security posture while supporting its commitment to excellence in education and safety. The adoption of facial recognition technology with algorithms like FaceNet represents a transformative step for API Banyuwangi in enhancing identity verification and security protocols. By embracing these technologies, the institution not only strengthens its defenses against security threats but also enhances operational efficiency and student safety. As technology continues to evolve, API Banyuwangi remains poised to leverage these advancements to maintain a secure and supportive environment for its educational community.

Facial recognition technology, particularly when integrated with advanced algorithms such as FaceNet, offers API Banyuwangi numerous benefits beyond security enhancement. The deployment of such technologies enables the institution to streamline various administrative processes, including attendance tracking, access control, and identity verification. By automating these tasks, API Banyuwangi can optimize resource allocation, reduce operational costs, and improve overall efficiency in managing campus facilities. Moreover, the implementation of facial recognition contributes to a more personalized and secure experience for cadets and staff alike. Through seamless authentication processes, individuals can access facilities and services with ease, minimizing disruptions and enhancing productivity. This convenience extends beyond security checkpoints to encompass various campus services, fostering a conducive environment for learning and collaboration.

Facial recognition's role in enhancing safety goes beyond traditional security measures. By integrating with other smart technologies, such as IoT-enabled surveillance systems or access management solutions, API Banyuwangi can create a comprehensive ecosystem that proactively monitors and responds to security threats in real-time. This proactive approach not only mitigates risks but also empowers administrators with actionable insights to optimize campus operations. Furthermore, the ethical considerations surrounding facial recognition deployment are critical for API Banyuwangi to address. Transparency in data handling, consent management, and privacy protection measures are essential to maintaining trust and compliance with regulatory requirements. By adopting best practices and adhering to ethical guidelines, the institution can ensure responsible use of facial recognition technology while safeguarding individual rights and freedoms.

Looking ahead, ongoing advancements in facial recognition technology hold promise for further innovation and refinement. Future developments may include enhanced accuracy through deep learning models, robust anti-spoofing measures, and expanded applications in personalized education services. These advancements position API Banyuwangi to continually enhance its security infrastructure while adapting to evolving educational needs and technological advancements.

The implementation of facial recognition technology at API Banyuwangi has significant social implications, particularly within the educational context. This technology can enhance administrative efficiency, such as speeding up identity verification processes and reducing manual workload. However, the social impact of this technology needs to be explored further to understand its implications for the educational community. Firstly, the use of this technology may alter the social dynamics on campus. With facial recognition, cadets and staff might experience increased surveillance, potentially affecting their sense of privacy and freedom. For instance, cadets might feel less comfortable with constant monitoring, which could impact their learning experience. Additionally, this technology could influence social relationships between cadets and staff if not implemented with transparency and clear communication.

Ethical issues are a major consideration in the implementation of facial recognition technology. Data security is a critical aspect, given that biometric information is highly sensitive personal data. Institutions must ensure that the facial data of cadets and staff is tightly protected and not misused. Consent is also an important issue; individuals should be clearly informed about the use of this technology and give their permission before their data is collected and used. Bias in facial recognition technology also needs to be addressed. This technology may exhibit varying accuracy based on ethnicity, gender, and age, which could lead to fairness issues. Therefore, it is important to choose technology that has been proven to be accurate and fair across different demographics and to implement policies that mitigate these biases.

In the long term, the implementation of this technology may affect the social structure at API Banyuwangi. If implemented well, it can enhance security and efficiency; however, if not managed carefully, it could lead to mistrust among cadets and staff. Long-term implications include changes in how cadets interact with each other and with staff, as well as how they perceive and respond to increased surveillance. Ongoing assessment of how this technology affects the campus community and how privacy and ethical policies are implemented is crucial to maintaining a balance between security and individual rights. Surveys and studies on user perceptions can provide additional insights into how this technology is received and its impact on social dynamics within the institution.

To address these challenges, it is crucial for policymakers at API Banyuwangi to establish a clear and comprehensive policy framework for the use of facial recognition technology. This policy should encompass several key aspects, including personal data protection, transparent consent processes, and strategies to mitigate bias. Specifically, policymakers should focus on ensuring transparency by clearly communicating to cadets and staff about the use of facial recognition technology, including its benefits and risks. Additionally, robust data protection measures must be implemented to safeguard biometric information from unauthorized access. Regular testing and evaluation of the technology are essential to ensure its accuracy and fairness, as well as to identify and address any potential biases. Finally, providing education and training for both staff and cadets on how the technology operates and how their privacy rights are protected will further enhance the ethical use of facial recognition technology. By adhering to these guidelines, API Banyuwangi can effectively use facial recognition technology in a manner that is both ethical and beneficial, while minimizing risks and negative impacts on the educational community.

In conclusion, the integration of facial recognition technology represents a transformative leap for API Banyuwangi in bolstering security, operational efficiency, and campus safety. By leveraging advanced algorithms like FaceNet, the institution not only strengthens its defenses against security threats but also enhances user experience and administrative effectiveness. As API Banyuwangi continues to evolve, embracing technological advancements in facial recognition underscores its commitment to providing a secure and innovative educational environment for its community.

## 4. Conclusion

The test results show that the performance of face recognition methods, particularly FaceNet, OpenFace, and Haar Cascade, varies significantly depending on the dataset used. FaceNet consistently demonstrates outstanding performance with high accuracy and low error rates, even when applied to complex datasets like FRGC. This makes FaceNet a highly reliable choice for applications that require high accuracy and the ability to handle a wide range of facial images. On the other hand, OpenFace, although not matching FaceNet in performance, still shows consistent and reliable results on the LFW and FRGC datasets. This consistency underscores OpenFace's robustness and its suitability for various applications that require dependable performance across different data scenarios.

However, the Haar Cascade method, while effective on the simpler LFW dataset, experiences a significant drop in performance when applied to the more challenging FRGC dataset. This notable decline in accuracy and increased error rate highlights the limitations of Haar Cascade in handling more complex and diverse facial data. Therefore, while Haar Cascade may be a viable option for simpler, more controlled environments, its use in more demanding applications is quite limited.

The implications of these findings for Digital Game-Based Learning (DGBL) are significant, especially in the context of user personalization and authentication. FaceNet, with its ability to manage complex datasets and deliver high accuracy, offers opportunities to enhance the user experience in DGBL environments by ensuring that user identities can be accurately recognized under various conditions. This can be applied to educational games that require reliable user authentication to provide content tailored to the user's profile. OpenFace can also be used in DGBL scenarios that require a balance between performance and efficiency, while Haar Cascade might be more suitable for simpler applications where facial data is less diverse.

The limitations of this study include the restricted scope of testing to three face recognition methods and two primary datasets. Additionally, the performance results achieved may not fully represent real-world situations, where variables such as lighting conditions, facial angles, and image resolution can affect the accuracy of facial recognition systems. Future research should expand the scope by testing other face recognition methods and using more diverse and realistic datasets to better understand how this technology can be effectively applied in real-world scenarios, particularly in the context of DGBL.

For future research, it is recommended to explore the integration of facial recognition technology with newer and more advanced deep learning techniques to enhance system accuracy and resilience. Additionally, further studies on how facial recognition can be integrated with other DGBL features, such as emotion analysis and user interaction, could provide deeper insights into improving the learning experience through better personalization. With this research direction, the contributions of this study can provide a strong foundation for developing more adaptive and efficient facial recognition systems, which will further support advancements in educational technology and game-based learning.

## Acknowledgment

We would like to acknowledge the contributions and support from various individuals and organizations in the course of this study on facial recognition technology. We extend our deepest gratitude to the API Banyuwangi for their cooperation and assistance in providing access to the necessary facilities and resources that were crucial for conducting our research. Their support was fundamental in ensuring that our study had the practical framework and logistical backing needed to succeed. Additionally, we are immensely grateful for the insightful discussions and guidance from our research advisors and colleagues. Their expertise, thoughtful critiques, and encouraging words significantly enriched the quality of this study, providing us with the direction and clarity needed to navigate complex research challenges. Without their continual support and constructive feedback, this research would not have achieved its depth and rigor. The collective efforts and collaborative spirit of all involved parties have been invaluable throughout the research process, underscoring the importance of teamwork and shared knowledge in advancing scientific inquiry.

## References

[1] M. Kulkarni, S. Tirupathi, P. Tirupathi, A. Abhang, and R. Deshmukh, “Smart Lab Management using Cloud and ML,” in 2023 6th International Conference on Advances in Science and Technology (ICAST), Dec. 2023, pp. 291–295, doi: 10.1109/ICAST59062.2023.10454949.

[2] S. Chinamanagonda, “Automating Cloud Governance - Organizations automating compliance and governance in the cloud,” MZ Comput. J., vol. 2, no. 1, pp. 1–16, May 2021. [Online]. Available at: http://mzjournal.com/index.php/MZCJ/article/view/341.

[3] M. A. Musarat, A. M. Khan, W. S. Alaloul, N. Blas, and S. Ayub, “Automated monitoring innovations for efficient and safe construction practices,” Results Eng., vol. 22, p. 102057, Jun. 2024, doi: 10.1016/j.rineng.2024.102057.

[4] L. Qinjun, C. Tianwei, Z. Yan, and W. Yuying, “Facial Recognition Technology: A Comprehensive Overview,” Acad. J. Comput. Inf. Sci., vol. 6, no. 7, pp. 15–26, 2023, doi: 10.25236/AJCIS.2023.060703.

[5] S. Zhou and S. Xiao, “Face Recognition System: a survey,” Human-centric Comput. Inf. Sci., vol. 8, no. 1, pp. 1-27, 2018, doi: 10.1186/s13673-018-0157-2.

[6] S. Gaur, M. Pandey, and Himanshu, “Realization of Facial Recognition Technology for Attendance Monitoring Through Biometric Modalities Employing MTCNN Integration,” SN Comput. Sci., vol. 5, no. 7, p. 862, Sep. 2024, doi: 10.1007/s42979-024-03225-1.

[7] M. Abdul-Al, G. Kumi Kyeremeh, R. Qahwaji, N. T. Ali, and R. A. Abd-Alhameed, “The Evolution of Biometric Authentication: A Deep Dive Into Multi-Modal Facial Recognition: A Review Case Study,” IEEE Access, vol. 12, pp. 179010–179038, 2024, doi: 10.1109/ACCESS.2024.3486552.

[8] M. Abdul-Al, G. K. Kyeremeh, R. Qahwaji, N. T. Ali, and R. A. Abd-Alhameed, “A Novel Approach to Enhancing Multi-Modal Facial Recognition: Integrating Convolutional Neural Networks, Principal Component Analysis, and Sequential Neural Networks,” IEEE Access, vol. 12, pp. 140823–140846, 2024, doi: 10.1109/ACCESS.2024.3467151.

[9] M. Aly, “Revolutionizing online education: Advanced facial expression recognition for real-time student progress tracking via deep learning model,” Multimed. Tools Appl., pp. 1–40, Jun. 2024, doi: 10.1007/s11042-024-19392-5.

[10] V. K. Patil, P. Nawade, R. Nagarkar, and P. Kadale, “Object Detection and Tracking Face Detection and Recognition,” in Integrating Metaheuristics in Computer Vision for Real-World Optimization Problems, Wiley, 2024, pp. 25–54, doi: 10.1002/9781394230952.ch2.

[11] X. Wang, Y. C. Wu, M. Zhou, and H. Fu, “Beyond surveillance: privacy, ethics, and regulations in face recognition technology,” Front. Big Data, vol. 7, p. 1337465, Jul. 2024, doi: 10.3389/fdata.2024.1337465.

[12] M. Wang and W. Deng, “Deep face recognition: A survey,” Neurocomputing, vol. 429, pp. 215–244, 2021, doi: 10.1016/j.neucom.2020.10.081.

[13] F. Firouzi et al., “Harnessing the Power of Smart and Connected Health to Tackle COVID-19: IoT, AI, Robotics, and Blockchain for a Better World,” IEEE Internet Things J., vol. 8, no. 16, pp. 12826–12846, Aug. 2021, doi: 10.1109/JIOT.2021.3073904.

[14] H. Omotunde and M. Ahmed, “A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond,” Mesopotamian J. CyberSecurity, vol. 2023, pp. 115–133, 2023, doi: 10.58496/MJCS/2023/016.

[15] W. Santoso, R. Safitri, and S. Samidi, “Integration of Artificial Intelligence in Facial Recognition Systems for Software Security,” sinkron, vol. 8, no. 2, pp. 1208–1214, Apr. 2024, doi: 10.33395/sinkron.v8i2.13612.

[16] S. H. Al Zaabi and R. Zamri, “Managing Security Threats through Touchless Security Technologies: An Overview of the Integration of Facial Recognition Technology in the UAE Oil and Gas Industry,” Sustainability, vol. 14, no. 22, p. 14915, Nov. 2022, doi: 10.3390/su142214915.

[17] M. I. A. Rohim et al., “Improving Face Recognition Performance on Low-Resolution Images Using Super-Resolution Method,” J. Teknol. Inf. dan Ilmu Komput., vol. 11, no. 1, pp. 199–208, 2024, doi: 10.25126/jtiik.20241117947.

[18] R. G. Guntara, “Facial Image Recognition Application on KTP Using Google Cloud Vision API and Kairos API Based on Android,” Ilk. J. Comput. Sci. Appl. Informatics, vol. 4, no. 2, pp. 198–207, 2022, doi: 10.28926/ilkomnika.v4i2.504.

[19] M. A. H. Akhand, S. Roy, N. Siddique, M. A. S. Kamal, and T. Shimamura, “Facial Emotion Recognition Using Transfer Learning in the Deep CNN,” Electronics, vol. 10, no. 9, p. 1036, Apr. 2021, doi: 10.3390/electronics10091036.

[20] L. A. W. Enforcement, U. S. E. Of, and F. R. Technology, “Face Off Law Enforcement Use Of Face Recognition Technology,” no. May, pp. 1–39, 2019, [Online]. Available at: https://www.eff.org/files/2019/05/28/face-off-report.pdf.

[21] M. Andrejevic and N. Selwyn, “Facial recognition technology in schools: critical questions and concerns,” Learn. Media Technol., vol. 45, no. 2, pp. 115–128, 2020, doi: 10.1080/17439884.2020.1686014.

[22] S. Wattamwar, R. Mate, P. Rainchwar, S. Mantri, and G. Sorate, “Optimal Face Recognition System using Haar Classifier,” in 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Oct. 2021, pp. 1–7, doi: 10.1109/SMARTGENCON51891.2021.9645879.

[23] M. Yousefi and E. Rajabi, “Digital Identity Verification Methods in Financial Services: Enhancing Security and Compliance,” Business, Mark. Financ. Open, vol. 1, no. 2, pp. 25–40, Mar. 2024,. [Online]. Available at: https://www.bmfopen.com/index.php/bmfopen/article/view/9.

[24] I. D. Raji, T. Gebru, M. Mitchell, J. Buolamwini, J. Lee, and E. Denton, “Saving Face: Investigating the ethical concerns of facial recognition auditing,” AIES 2020 - Proc. AAAI/ACM Conf. AI, Ethics, Soc., pp. 145–151, 2020, doi: 10.1145/3375627.3375820.

[25] S. Rahman, E. F. Aliff S, and A. M. Elhanafi, "Face Recognition Application Using Backpropagation Algorithm and Voila Jones," J. Teknol. dan Ilmu Komput. Prima, vol. 1, no. 1, pp. 91–101, 2018, doi: 10.34012/jutikomp.v1i1.336.

[26] A. S. Nikolaev, T. G. Maximova, I. E. Sakhno, A. A. Antipov, and S. V. Murashova, "Facial Recognition Technologies Patent Landscape," in Lecture Notes in Networks and Systems, vol. 596 LNNS, Springer, Cham, 2023, pp. 568–583, doi: 10.1007/978-3-031-21435-6_49.

[27] X. Cheng, L. Qiao, B. Yang, and X. Zhang, "Investigation on users' resistance intention to facial recognition payment: a perspective of privacy," Electron. Commer. Res., vol. 24, no. 1, pp. 275–301, Mar. 2024, doi: 10.1007/s10660-022-09588-y.

[28] S. P. Putra, I. Fitri, and S. Ningsih, "Facial Recognition Attendance Using Web-Based Eigenface Algorithm," J. Appl. Informatics Comput., vol. 5, no. 1, pp. 21–27, 2021, doi: 10.30871/jaic.v5i1.2711.

[29] D. Satria, "Analysis and Implementation of Association Rule with Apriori Algorithm in Accepting Lecturers Case Study at (Stkip) Ypm Bangko," J. Teknol. Dan Sist. Inf. Bisnis, vol. 2, no. 2, pp. 74–85, 2020, doi: 10.47233/jteksis.v2i2.117.

[30] M. Sari, H. Rachman, N. Juli Astuti, M. Win Afgani, and R. Abdullah Siroj, "Explanatory Survey dalam Metode Penelitian Deskriptif Kuantitatif," J. Pendidik. Sains dan Komput., vol. 3, no. 01, pp. 10–16, 2022, doi: 10.47709/jpsk.v3i01.1953.

[31] M. D. Choudhry, S. Munusamy, J. Sivaraj, and A. Jothi, "Fundamentals of Statistics," in Quantum Machine Learning, Boca Raton: Chapman and Hall/CRC, 2024, pp. 3–30, doi: 10.1201/9781003429654-2.

[32] J. B. Grace and K. M. Irvine, "Scientist's guide to developing explanatory statistical models using causal analysis principles," Ecology, vol. 101, no. 4, p. e02962, Apr. 2020, doi: 10.1002/ecy.2962.

[33] V. Mutneja and S. Singh, "Haar-features training parameters analysis in boosting based machine learning for improved face detection," Int. J. Adv. Technol. Eng. Explor., vol. 8, no. 80, pp. 919–931, Jul. 2021, doi: 10.19101/IJATEE.2021.874076.

[34] S. O. Adeshina, H. Ibrahim, S. S. Teoh, and S. C. Hoo, "Custom Face Classification Model for Classroom Using Haar-Like and LBP Features with Their Performance Comparisons," Electronics, vol. 10, no. 2, p. 102, Jan. 2021, doi: 10.3390/electronics10020102.

[35] T. Q. Vinh and N. T. N. Anh, "Real-Time Face Mask Detector Using YOLOv3 Algorithm and Haar Cascade Classifier," Proc. - 2020 Int. Conf. Adv. Comput. Appl. ACOMP 2020, pp. 146–149, 2020, doi: 10.1109/ACOMP50827.2020.00029.

[36] M. Sitorus and Nurul Fadillah, "Multi Face Detection System Using Haar Cascade Classifier Method," J-ICOM - J. Inform. dan Teknol. Komput., vol. 1, no. 1, pp. 1–5, 2020, doi: 10.33059/j-icom.v1i1.2728.

[37] A. Sehanobish, N. Ravindra, and D. van Dijk, "Gaining Insight into SARS-CoV-2 Infection and COVID-19 Severity Using Self-supervised Edge Features and Graph Neural Networks," 35th AAAI Conf. Artif. Intell. AAAI 2021, vol. 6A, pp. 4864–4873, 2021, doi: 10.1609/aaai.v35i6.16619.

[38] M. P. Véstias, "A survey of convolutional neural networks on edge with reconfigurable computing," Algorithms, vol. 12, no. 8, pp. 1-24, 2019, doi: 10.3390/a12080154.

[39] A. Singh, H. Herunde, and F. Furtado, "Modified Haar-Cascade Model for Face Detection Issues," Int. J. Res. Ind. Eng. , vol. 9, no. 2, pp. 143–171, 2020. [Online]. Available at: https://www.riejournal.com/article_107190.html.

[40] H. Jeong, G. R. Kwon, and S. W. Lee, "Deterioration Diagnosis of Solar Module Using Thermal and Visible Image Processing," Energies, vol. 13, pp. 1–14, 2020, doi: 10.3390/en13112856.

[41] Prof. Dr. Paul Mccullagh, "Face detection by using Haar Cascade Classifier," Wasit J. Comput. Math. Sci., vol. 2, no. 1, pp. 1–5, Mar. 2023, doi: 10.31185/wjcm.109.

[42] D. Junaidy, M. Wulandari, and H. Tanudjaja, "Real time face detection using haar-like feature method and local binary pattern method," IOP Conf. Ser. Mater. Sci. Eng., vol. 508, no. 1, pp. 1-6, 2019, doi: 10.1088/1757-899X/508/1/012076.

[43] J. L Gaol, M. Rivai, and T. Tasripan, "Biometric Authentication System based on Electroencephalography Signal Spectrum Features," J. Tek. ITS, vol. 7, no. 2, pp. 337, 342, 2019. [Online]. Available at: https://www.neliti.com/publications/497226/sistem-autentikasi-biometrik-berbasis-fitur-spektrum-sinyal-elektroensefalografi.

[44] R. Solekha, M. Alif Ramadhan, F. Nurdiyanto, and U. Latifa, "Fector : Face Emotion Detector Sebagai Penunjang Efektivitas Dalam Pembelajaran Daring (Dalam Jaringan)," JATI (Jurnal Mhs. Tek. Inform., vol. 8, no. 2, pp. 2047–2055, 2024, doi: 10.36040/jati.v8i2.7962.

[45] M. Ebrahimi Kalan, R. Jebai, E. Zarafshan, and Z. Bursac, "Distinction Between Two Statistical Terms: Multivariable and Multivariate Logistic Regression," Nicotine Tob. Res., vol. 23, no. 8, pp. 1446–1447, Aug. 2021, doi: 10.1093/ntr/ntaa055.

[46] A. Das, "Logistic Regression," in Encyclopedia of Quality of Life and Well-Being Research, Cham: Springer International Publishing, 2023, pp. 3985–3986, doi: 10.1007/978-3-031-17299-1_1689.