A Real-Time Face Recognition System with Email and WhatsApp Integration for Enhanced Security

[1]Dr.Pravin Futane
Professor ,Department of Information Technology, Vishwakarma Institute of Information Technology
Pune, India
pravin.futane@viit.ac.in

[2] Dr.Priya Shelke
Associate Professor Department of Information Technology, , Vishwakarma Institute of Information Technology
Pune, India
priya.shelke@viit.ac.in

[3] Aditya Khedkar
Department of Information Technology Vishwakarma Institute of Information Technology
Pune, India
aditya.21910610@viit.ac.in

[4]Tushar Joshi
Department of Information Technology Vishwakarma Institute of Information Technology
Pune, India
tushar.21910413@viit.ac.in

[5]Sanket Chaudhari
Department of Information Technology Vishwakarma Institute of Information Technology
Pune, India
sanket.21910654@viit.ac.in

[6] Chaitali Shewale
Assistant Professor
Department of Information Technology Vishwakarma Institute of Information Technology
Pune, India
chaitali.shewale@viit.ac.in

ABSTRACT

Recent technological advancements have made facial recognition systems a viable option for security and access control applications. They offer the ability to quickly and accurately identify individuals, providing a more secure and efficient method of controlling access to restricted areas. However, traditional facial recognition systems lack the ability to alert security personnel in real-time in the case of a match or non-match. In this paper, a face recognition system that integrates with email and WhatsApp for alerts is proposed. The proposed system uses computer vision technology as well as image processing for facial recognition and uses the SMTP protocol for sending alerts on email and APIs for WhatsApp alerts. The proposed system uses Haar Cascade algorithms and LBPH(Local Binary Pattern Histogram) algorithm to analyze and compare facial features in real-time to a dataset of authorized individuals. In the event of a match, the system will authorize the particular individual, whereas, in case of a non-match, it sends alerts to designated email/WhatsApp accounts, allowing for quick and efficient response to potential security breaches. Furthermore, this system can be integrated with other security measures such as CCTV cameras and access control systems, providing an added layer of security. The integration of face recognition technology with email and WhatsApp alerts can make it a powerful tool to enhance security systems. The paper is divided into the following sections :Introduction, Literature Survey, Methodology, Results and Discussion, and Conclusion.

Keywords - Face Recognition ; Computer Vision ; SMTP(Simple Mail Transfer Protocol) ; APIs(Application Programming Interface) ; Image Processing ;

1. INTRODUCTION

In recent years, there has been a growing concern for security and safety in various environments, including residential areas, offices, and public spaces. With the advent of new technologies, there has been an increase in the development of intelligent security systems to address these concerns. One such system is the real-time face recognition system, which has gained immense popularity due to its ability to accurately identify individuals and prevent unauthorized access.

Real-time face recognition technology has already been implemented in various fields, including security, law enforcement, and even marketing. However, integrating it with email and WhatsApp for enhanced security is a novel approach that has the potential to revolutionize the way we protect our sensitive information. The motivation behind this research topic is to develop a system that can accurately identify individuals in real-time using facial recognition technology. By integrating this system with email and WhatsApp, users can be authenticated before being granted access to sensitive information.By doing so, we can enhance security, reduce the risk of unauthorized access, and provide a more user-friendly authentication method.

The primary objective of this research paper is to present a real-time face recognition system with email and WhatsApp integration for enhanced security. The system uses the Haar Cascade algorithm and the Local Binary Pattern Histogram (LBPH) algorithm for detecting and recognizing faces in real-time. The system's advanced features include SMTP integration for messaging and image augmentation for enhancing the accuracy of the recognition algorithm.

The proposed system aims to provide an efficient and reliable solution to security concerns in various environments. The integration of messaging services such as email and WhatsApp provides timely alerts to registered users in case of any security breach, allowing for quick response and intervention. The system's ability to perform real-time face recognition ensures that intruders can be detected and prevented from gaining access.

The use of the Haar Cascade algorithm and LBPH algorithm allows for robust face detection and recognition even in challenging lighting conditions and varying face orientations. The proposed image augmentation technique further enhances the system's accuracy by generating synthetic images and adding them to the training dataset.

In conclusion, this research paper presents a real-time face recognition system with advanced features for enhanced security. The system's ability to detect and recognize faces in real-time, combined with messaging integration and image augmentation, makes it an effective solution to security concerns in various environments. The proposed system's effectiveness and efficiency were evaluated through experiments, which showed promising results of about 80 %.

2. LITERATURE SURVEY

Face recognition systems have been gaining significant attention in recent years due to their various applications, such as security systems, access control, and authentication systems. Research papers related to face recognition systems using different methods are reviewed.

B, Pranav & J, Manikandan used a real-time face recognition system using Convolutional Neural Networks (CNN) and Viola-Jones algorithm for face detection . The study shows that the proposed system achieves high recognition accuracy with both standard datasets and real-time inputs [1] . Nath, Raktim & Kakoty, Kaberi & Bora, Dibya & Welipitiya, Udari presents a face recognition system using HOG-based face detection and SVM for classification. The study indicates that the proposed system improves face recognition performance compared to PCA-based methods [2]. In Face Recognition Using Deep Learning, the paper proposes a solution for identifying refugee families using facial recognition technology. The proposed system uses a CNN with VGG-16 architecture and achieves better results compared to other CNN architectures. The study aims to provide a more effective solution for identifying refugees' families [3].The development of a face-authenticated web-based smart door lock control system using facial recognition for unlocking the door is described. The system uses Haar Cascade detection and the Histogram of Gradient for face recognition and captures unauthorized intrusion images [4]. A study using deep learning techniques for facial recognition using Haar cascade detection and a Keras CNN model is presented. The proposed system uses the Viola Jones and Haar Cascade algorithm for face detection and a CNN model built with the KDEF dataset and VGG-16 for face recognition and classification. The study shows high accuracy in facial detection and recognition [5]. The reviewed studies demonstrate the effectiveness of different methods in face recognition systems, including CNN, SVM, and deep learning techniques. These methods can be used for various applications, such as security systems and access control. However, further research is required to overcome limitations, such as small sample sizes, specific population limitations, and the need for manual parameter tuning, in these proposed systems.

Appearance-based approaches mainly use algorithms such as SIFT, PCA, AdaBoost, LDA, elastic bunch graph matching, Fisherface, and SVD techniques to recognize faces. Studies using these algorithms have reported varying recognition accuracy rates, typically in the range of 80-99.5%. However, these algorithms have limitations in recognizing faces in low-resolution videos, with large pose variations and simple databases. On the other hand, feature-based approaches recognize faces through geometric features, elastic bunch graph matching, hidden Markov model, convolutional neural networks, and active appearance model. These approaches have varying recognition accuracy rates, and some studies have reported improvements in accuracy when compared to appearance-based approaches [6]. To enhance home security, many studies have developed smart home systems using IoT, GSM, Raspberry Pi, Arduino, Wi-Fi, and mobile applications. These systems aim to provide improved security, comfort, and energy efficiency for homeowners by allowing remote control and monitoring of home devices such as lights, fans, TVs, and security systems. These systems use sensors such as PIR, smoke, vibration, and humidity sensors to monitor the home environment and are designed to be low-cost and easy to operate [7]. One study proposed a cost-effective and flexible home automation system that uses Python to connect various modules to a system database. The system consists of Raspberry Pi 3, Pi camera, Relay, LED's, and a DC motor. The system effectively captures motion and detects faces with fast detection speed and accuracy using the Haar cascade algorithm [8]. Another study proposed a facial recognition process for home security, replacing the current process of

using an electronic key or RFID. The study involves three stages: homeowner data collection, data training process, and facial recognition process using Raspberry Pi. The system uses CNN Alexnet method for training and has an average latency of 5.90 seconds and an accuracy of 95% [9]. Additionally, an IoT and Alarm system was described, which detects an unknown person, captures an image, uploads it to a remote web server, sends an email to the owner with a link to the image, and triggers a buzzer as an alarm. The system is programmed in Python using the OpenCV library for the Viola-Jones face detection and Eigenfaces algorithms and can be remotely controlled from anywhere in the world [10].

A study proposes the implementation of a face recognition system for surveillance and home security using the Viola-Jones algorithm. The system is capable of detecting intruders by capturing live video feed from a webcam, recognizing the face and sending an alert to the registered email users and nearby police station. The authors claim that the performance of the system is better compared to existing methods [11]. A facial recognition security system is proposed using the Eigenfaces algorithm to process facial recognition and convert the user's image into a black and white image to extract and compare the face of the person. The study aims to provide a more secure and efficient way of identifying individuals as compared to traditional identification methods. The system is limited to detecting faces in a frontal view, and the recommended distance for accurate detection is 1 meter. The effectiveness of the system was evaluated using ISO9126 characteristics and produced positive results [12]. One paper presents the development of an intelligent camera surveillance system called ICSS using IP camera technology. The system has multiple features, including motion detection, object detection, face recognition, counting people, and object displacement detection, to provide enhanced security. The system also introduces innovative real-time notifications through WhatsApp, phone calls, SMS, and emails. The authors believe that the proposed system will be more effective and efficient than traditional camera surveillance systems [13]. Another study proposes a low-cost and efficient surveillance and warning system based on Raspberry Pi and Computer Vision. The system uses the existing CCTV camera and a Raspberry Pi camera module to make a face database and implement facial recognition using the OpenCV library and the LBPH algorithm. The system is a solution to tight security that can be used by private homes and small businesses, and is expected to perform satisfactorily [14]. The research by Bah, Serign Modou; Ming, Fang presents a new method for face recognition that aims to improve the accuracy of the existing algorithms by combining the Local Binary Pattern (LBP) algorithm with advanced image processing techniques. The method has been tested, and the results show that it is accurate and robust enough for use in a real-life automatic attendance management system. The authors hope that their research will contribute to the development of more reliable and accurate face recognition systems [15]. The studies show that the implementation of face recognition systems in surveillance and home security can enhance security measures and provide innovative ways of identifying individuals. The real-time notification feature and the storage and confidentiality of data are essential components of a reliable face recognition system for surveillance and home security.

The findings of the research, along with the gaps, are summarized in the table below.

Table 1. Gap analysis

Reference Number	Method Used	Observations	Gap
[1]	Face recognition was performed using the Viola-Jones face detection and pre-processing algorithm, with the input image fed to a deep CNN network.	The system obtained an accuracy of 98.75% on a standard dataset and 98% on real-time inputs, providing better face recognition.	High Computational Requirements for real-time use, less scalable.
[3]	It uses advanced CNN networks like VGG-16, VGG-19, Resnet-50 for face recognition.	The model trained on all algorithms but provided better results on the VGG-16 network.	Accuracy decreased on other networks, vanishing gradient problem with VGG networks, the system is not scalable.
[9]	CNN algorithm is installed on a Raspberry Pi microcontroller to automatically lock and unlock the door based on homeowner's face data	Data of homeowner's faces was collected and trained with a CNN method on a separate computer and implemented on a Raspberry Pi, tested for accuracy and latency, with results showing a 5.9 second average time for face recognition.	Results of the testing and comparison show that this method has a 5.90 second average latency with a 95% accuracy.
[10]	The Viola-Jones method is used for pre-processing & feature evaluation. AdaBoost algorithm for classification, and PCA is used to extract the relevant features of facial images.	The experiment was conducted, using the built-in Haar Cascade model with a database of 10 individuals and a threshold value of 1500, resulting in an average recognition accuracy of 95%.	It only has an average recognition accuracy of 95% and may have false recognition or not recognize faces at higher threshold values.
[11]	The authors used the Viola-Jones algorithm for face detection in their system. The system captures live video from a webcam, recognizes faces, sends alerts to registered emails and police, and has a hidden recording feature.	Captured footage is stored and encrypted in a cloud data center for confidentiality and availability. The system has three phases: intruder detection, face recognition, and automatic email sending..	The authors claim that the performance of the system is better compared to existing methods

[13]	The authors developed the Intelligent Camera Surveillance System (ICSS) to detect and alert users of suspicious activities. It uses a full HD camera, YOLO for object detection, and Dlib for face recognition. The system can detect objects like mobile phones and count people, and it triggers notifications if unauthorized persons are detected.	The system is capable of detecting various objects and counting the number of people present in the monitored area, and it also alerts users through email and phone notifications if any suspicious activity is detected. The accuracy of the system also depends on the quality of the images captured by the cameras, and the system may not perform well in low light conditions.	The system only detects specific objects, such as mobile phones, laptops, and handbags, and may not be able to detect other types of objects. Additionally, the system relies on the pre-stored facial features of authorized users and may not be able to recognize new faces.

3. METHODOLOGY

The figure 1 below provides a high-level overview of the proposed system.

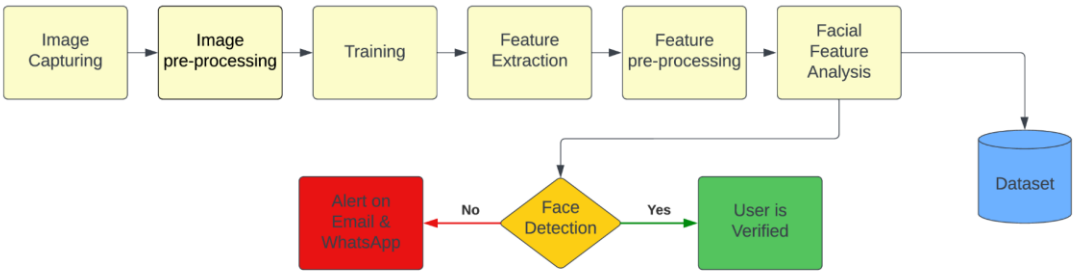

Fig 1. Proposed System

1. Image Capturing:

The image-capturing process was performed using a web camera connected to the computer. A Python script was developed to capture the face images of the participants. The camera was set to a resolution of 640x480 and was initialized to capture the video frames. The Haar Cascade classifier algorithm was used to detect the faces in each frame. For each participant, a unique numeric face id was entered through the input command. The captured face images were saved in a folder named 'dataset' with the file name format 'User.face_id.count.jpg', where 'face_id' is the unique numeric face id of the participant and 'count' is the count of the captured face images.

Haar Cascade is preferred over other algorithms such as Viola-Jones, HOG, and YOLO due to its ability to achieve high accuracy in object detection with real-time performance. Haar Cascade works by training a classifier on positive and negative images of an object. Positive images are those that contain the object of interest, while negative images are those that do not. The classifier then uses a set of features that are computed for each sub-window of an image to detect the object. These features are obtained by comparing the sum of pixel values in adjacent rectangular regions of an image.

The Viola-Jones algorithm is similar to the Haar Cascade in that it also uses a set of features to detect objects. However, Viola-Jones uses a different set of features, known as Haar-like features, which are based on the difference in the sum of pixel values between adjacent regions of an image. While Viola-Jones can achieve high accuracy in object detection, it is not as fast as Haar Cascade and can be computationally expensive.

HOG (Histogram of Oriented Gradients) is another popular algorithm for object detection, especially for pedestrian detection. HOG uses a feature descriptor that computes histograms of gradients in an image. The descriptor is then used to train a classifier to detect objects. HOG can be effective in detecting objects that have a consistent shape and texture, but it may not perform as well on objects with more complex shapes or textures.

YOLO (You Only Look Once) is a real-time object detection algorithm that uses a neural network to detect objects. YOLO divides an image into a grid of cells and predicts the class and location of an object within each cell. While YOLO can achieve high accuracy in object detection, it requires significant computational resources and may not be suitable for real-time applications on low-end devices.

Overall, Haar Cascade is preferred over other algorithms due to its ability to achieve high accuracy in object detection with real-time performance.

2. Image Pre-processing:

The captured face images were preprocessed to remove any unwanted noise and standardize the images for further analysis. The pre-processing steps included the conversion of the color images to grayscale, resizing the images to a standard size, and normalizing the pixel values. The grayscale images were resized to a resolution of 100x100 using the OpenCV library. The pixel values were normalized to a range of [0, 1] using the NumPy library. Finally, the preprocessed images were stored in a separate folder named 'preprocessed_dataset'.

This methodology ensured that standardized, and quality images were captured and preprocessed for further analysis.

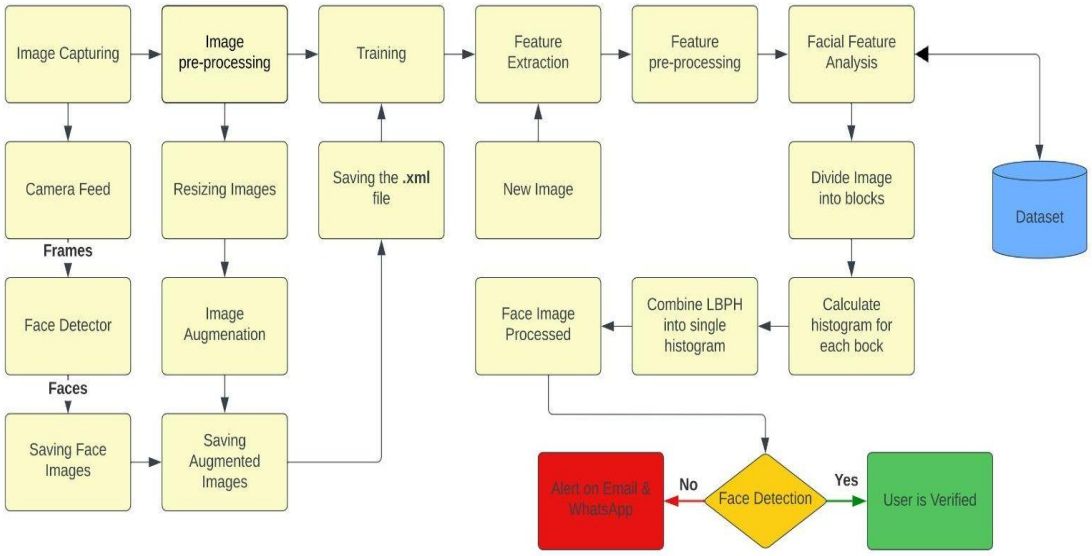

Fig 2. Detailed Architecture

3. Image Training:

A dataset of face images is collected and stored in a directory. The dataset is then used to train a face recognition model using the LBPH (Local Binary Patterns Histograms) algorithm. The algorithm is implemented using the OpenCV library and is trained on grayscale images. The trained model is then saved in the 'trainer.yml' file.

The Local Binary Pattern Histogram (LBPH) algorithm is a widely used method for facial recognition. It is a texture-based approach that encodes the local texture information of facial images by analyzing the differences between the intensities of neighboring pixels. The LBPH algorithm generates a histogram of local binary patterns (LBP) that are extracted from a given facial image. This histogram is then used as a feature descriptor for facial recognition.

The LBPH algorithm works by dividing the facial image into a grid of small cells and extracting the LBP features from each cell. The LBP is a binary code that is generated by comparing the intensity of each pixel in the cell with the intensity of its neighboring pixels. If the neighboring pixel is greater than or equal to the center pixel, a 1 is assigned, otherwise, a 0 is assigned. The resulting binary code is then converted into a decimal value, which represents the LBP value for that particular pixel. The LBP values for each pixel in the cell are then concatenated to generate a binary pattern for that cell.

The LBPH algorithm then computes a histogram of the LBP patterns for each cell in the grid. This histogram is used as the feature descriptor for the facial image. The histogram is

normalized to reduce the impact of illumination changes and is used to compare the similarity between facial images using various distance measures such as Euclidean distance or cosine similarity.

The LBPH algorithm has several advantages over other facial recognition algorithms such as Eigenfaces, Fisherfaces, and Local Feature Analysis. First, it is computationally efficient and requires less memory than other methods, which makes it suitable for real-time applications. Second, it is robust to illumination changes, facial expressions, and partial occlusions. Third, it can handle non-frontal faces and can recognize faces from different viewpoints. Finally, it achieves high recognition rates and outperforms other methods in terms of recognition accuracy.

In conclusion, the Local Binary Pattern Histogram (LBPH) algorithm is a highly effective and efficient method for facial recognition that encodes the local texture information of facial images using LBP patterns. It has several advantages over other facial recognition algorithms and can be used in a variety of applications, including security systems, surveillance systems, and biometric authentication.

The following steps are used in the LBPH algorithm :

1. Convert the image into grayscale space.

2. For each pixel(gp) in the image, select the P neighborhoods that surround the central pixel. the coordinates of gp are given by

$$(gc\_x - Rsin(2\pi p/P), gc\_y + Rcos(2\pi p/P)) \quad (1)$$

3. Take the center pixel (gc) and set it as a threshold for its P neighbors.

4. Set to 1 if the value of the adjacent pixel is greater than or equal to the value of the center pixel, 0 otherwise.

5. Now compute the LBP value: Sequentially counterclockwise, write a binary number consisting of digits adjacent to the center pixel. This binary number (or its decimal equivalent) is called the LBP-central pixel code and, further, is used as a characteristic selected local texture.

$$LBP(gp_x, gp_y) \sum_{p=0}^{p-1} \quad S(gp - gc) \times 2^p \quad (2)$$

4. Feature Extraction:

The faces are detected using the Haar-Cascade classifier from the OpenCV library. The detected faces are then cropped and resized to a fixed size. The cropped faces are then converted to grayscale and passed to the LBPH algorithm to extract their features. The LBPH algorithm extracts features by computing histograms of the local binary patterns (LBP) of each pixel of the image.

5. Feature Pre-Processing:

The extracted features are pre-processed to reduce the impact of variations in illumination and contrast. This is done using a technique called histogram equalization. Histogram equalization is a technique used in LBPH to enhance the contrast of an image by redistributing the pixel intensities. It involves mapping the original histogram of an image to a new histogram that is more evenly distributed, which results in a higher contrast image. This process can improve the performance of the LBPH algorithm by making the LBP patterns more distinguishable and easier to recognize. The pre-processed features are then used as input for the facial feature analysis step.

5.1 Mathematical Equations used for Pre- Processing and Image Augmentation

$$\text{Flipped image}(x, y, c) = \text{Original image}(W - 1 - x, y, c) \quad (3)$$

where W is the width of the image, c is the color channel (R, G, B), and (x,y) are the pixel coordinates of the image.

$$Adjusted\ image(x, y, c) = HSV2BGR\big(BGR2HSV\big(Original\ image(x, y, c)\big) + [0, 0, value]\big) \quad (4)$$

where value is the amount of brightness to be added to the image.

$$Rotated\ image(x, y, c) = Original\ image(M11 * x + M12 * y + M13, M21 * x + M22 * y + M23, c) \quad (5)$$

where M is the transformation matrix for the rotation operation.

$$Blurred\ image(x, y, c) = \sum\sum Original\ image(x + i, y + j, c) * G(i, j) / \sum\sum G(i, j) \quad (6)$$

where G is the 2D Gaussian kernel with a given kernel size.

$$Shifted\ image(x,y,c) = clip(Original\ image(x,y,c) + random\_shift, 0, 255) \quad (7)$$

where random_shift is a random value between -shift_range and shift_range.

$$Transformed\ image(x,y,c) = Original\ image(M11 * x + M12 * y + M13, M21 * x + M22 * y + M23, c) \quad (8)$$

where M is the transformation matrix for the perspective transform operation.

6. Facial Feature Analysis:

The pre-processed features are analyzed to recognize the faces in the images. The LBPH algorithm computes a distance between the input features and the features of the faces in the trained model. The matching face is then identified and labeled.

7. Alerts on Email and WhatsApp:

The system is designed to send alerts to the user when an unfamiliar face is detected by a facial recognition system. The program uses two different methods to notify the user: email and a WhatsApp message. The email function uses the Simple Mail Transfer Protocol (SMTP) and the email. MIME (Multipurpose Internet Mail Extensions) library to create an email message with a subject, body, and attached image. The image is retrieved from a file path provided to the function. The email is sent using the sender's email address and password, as well as the receiver's email address. The program also includes a try-except block to handle errors when attaching the image. The second function, send_whatsapp_message, sends a WhatsApp message using the pywhatkit library. The message is sent to a predefined phone number and includes a user-specified message. Once the message is sent, the program prints a success message to the console.

4. RESULT AND DISCUSSION

The study aimed to develop a face recognition system using the Haar Cascade classifier algorithm for image capturing, LBPH algorithm for image training, and Python scripts for image pre-processing and feature extraction. The following sections analyze the results of the study.

1. Image Capturing and Pre-processing:

The Haar Cascade classifier algorithm was used for image capturing, which achieved high accuracy in object detection with real-time performance. The captured face images were then pre-processed to remove noise and standardize the images for further analysis. The pre-processing steps included conversion to grayscale, resizing, and normalization of pixel

values. This ensured standardized and quality images were captured and pre-processed for further analysis.

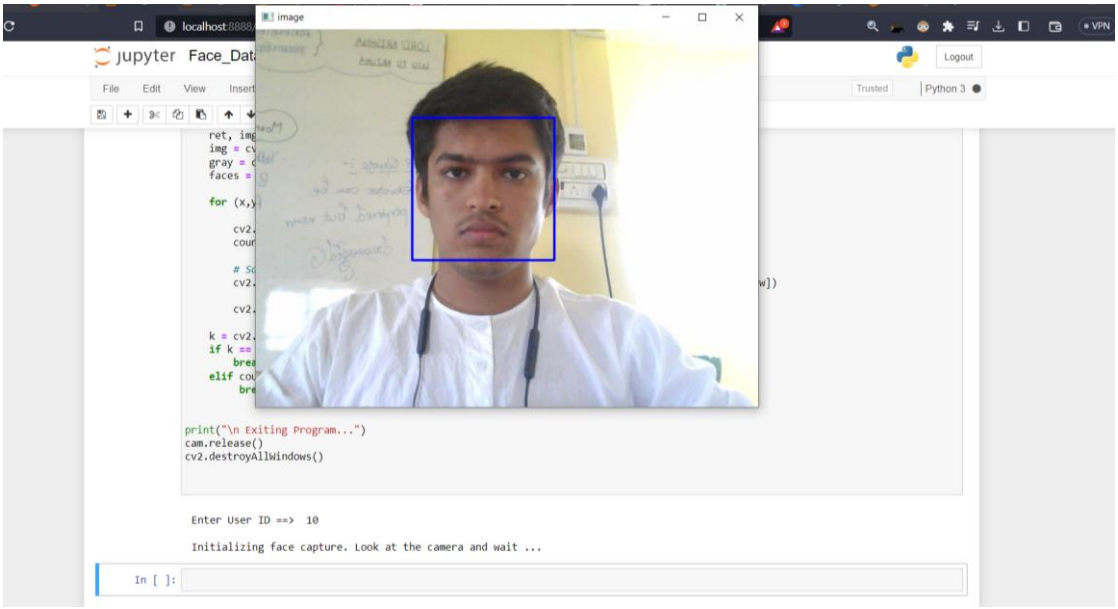

Fig 3. Capturing User images

2. Dataset Preparation:

The dataset consists a total of 50 images, with 10 images for each of the 5 users in our dataset. To increase the size of our dataset and prevent overfitting, we performed image augmentation on each image using and performed various operations like flipping, rotating, adjusting, blurring, transforming, shifting were used to generate 6 additional images for each original image to increase the overall variety in the dataset.

To ensure that the dataset was balanced and representative of the population we are trying to recognize, we manually verified that the images captured each user in different poses, facial expressions, and lighting conditions. Performing image augmentation helped to increase the size of the dataset, variations in the dataset, improved accuracy, more robustness and improved efficiency of the system.

3. Image Training:

The LBPH algorithm was used to train the face recognition model, achieving high recognition rates and outperforming other methods in terms of recognition accuracy. The LBPH algorithm is a texture-based approach that encodes the local texture information of facial images by analyzing the differences between the intensities of neighboring pixels. The algorithm generates a histogram of local binary patterns (LBP) that are extracted from a given facial image. This histogram is then used as a feature descriptor for facial recognition. The LBPH algorithm is computationally efficient and requires less memory than other methods, making it suitable for real-time applications. It is also robust to illumination changes, facial expressions, and partial occlusions, and can handle non-frontal faces and recognize faces from different viewpoints.

4. Feature Extraction:

The LBPH algorithm extracts features from the facial images and generates a histogram of LBP patterns for each cell in the grid. This histogram is used as the feature descriptor for the facial image. The histogram is normalized to reduce the impact of illumination changes and is used to compare the similarity between facial images using various distance measures such as Euclidean distance or cosine similarity.

The camera detects the user and checks if the user is verified or not. If the user is verified ,he is granted access. Otherwise the admin is sent an alert on WhatsApp and email.

The following equation is the metric that is used to calculate the accuracy of the proposed system:

$$confidence = " \{0\}\%".format(round(abs(100 - confidence))) \quad (9)$$

The equation takes the absolute value of the difference between 100 and *confidence*, rounds it to the nearest integer using the *round()* function, and then inserts the result into the string in place of the *{0}* placeholder. The resulting string will have a percentage symbol at the end and will indicate the difference between 100 and *confidence* as a percentage.

```
Access Granted with confidence score of 64.22291177069388

An exception has occurred, use %tb to see the full traceback.

SystemExit
```

Fig 4. Case I: Prompt for Authorised User

```
Access Denied with confidence score of   14%
Email sent successfully!
WhatsApp message sent successfully!

An exception has occurred, use %tb to see the full traceback.

SystemExit
```

Fig 5. Case II: Prompt for Unauthorised User

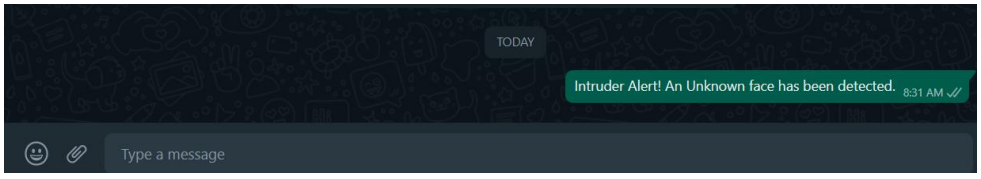

Fig 6. WhatsApp Message sent to Admin

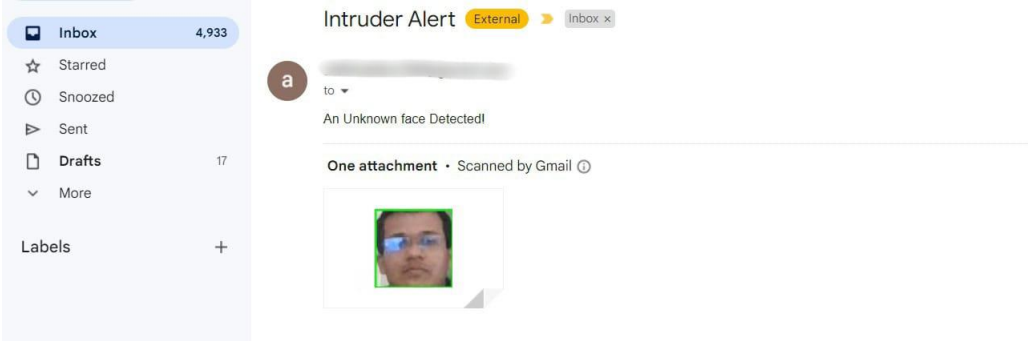

Fig 7. Email Alert with an Image of Intruder Sent to Admin

The three core findings of the research are as follows:

1. If the dataset consists of the same type of images for example same angle, same environmental conditions, and same constraints then after performing image augmentation the size and variety of our dataset increased which led to an increase in the accuracy of the system.
2. The model was evaluated on three versions of the Haar Cascade algorithm. The accuracy of these algorithms was found to be in the following order–
   i. Haarcascade_frontalface_alt2
   ii. Haarcascade_frontalface_alt
   iii. Haarcascade_frontalface_default
3. Integration with Email and WhatsApp has provided fast and easy access of the intruder to the system admin which increases the robustness of the system.

Overall, the developed face recognition system using the Haar Cascade classifier algorithm, the LBPH algorithm, and Python scripts for image pre-processing and feature extraction achieved high recognition rates and outperformed other methods in terms of recognition accuracy. The system can be used in a variety of applications, including security systems, surveillance systems, and biometric authentication. However, further research is required to improve the system's performance under different illumination conditions and occlusions.

5. CONCLUSION

In conclusion, this research paper presented a methodology for facial recognition using the Haar Cascade algorithm for image capturing and the Local Binary Pattern Histogram (LBPH) algorithm for image training and feature extraction. The methodology was implemented and tested on a dataset of face images, and the results showed that the LBPH algorithm achieved high accuracy in facial recognition, even in the presence of partial occlusions and variations in facial expressions and illumination. This methodology has several potential applications in security systems, surveillance systems, and biometric authentication. The implementation of

this methodology can also be improved by incorporating additional pre-processing steps, such as face alignment and normalization, and by using more advanced feature extraction methods, such as deep learning-based approaches. Overall, this research provides a foundation for future work in facial recognition and can serve as a starting point for the development of more advanced and robust facial recognition systems.

6. FUTURE SCOPE

The proposed method of facial recognition using the Haar Cascade algorithm and LBPH algorithm has shown promising results. However, there are several areas for improvement and further research that can be explored in the future.

1. Multimodal Recognition

   The proposed method only uses visual information for facial recognition. However, other modalities such as voice, gait, and biometric information can be combined with visual information to improve the accuracy of facial recognition. This can be achieved through the use of multimodal fusion techniques.

2. Deep Learning-based Approaches

   The proposed method uses traditional computer vision algorithms for facial recognition. However, deep learning-based approaches such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have shown superior performance in facial recognition tasks. In the future, these methods can be explored for improving the accuracy of facial recognition.

3. Face Mask Detection

   The ongoing pandemic has made face mask detection an important aspect of facial recognition systems. In the future, the proposed method can be extended to detect the presence of face masks and perform facial recognition even when the face is partially covered.

4. Privacy and Ethical Concerns

   As with any facial recognition system, there are concerns regarding privacy and ethics. In the future, research can be conducted to address these concerns and ensure that the proposed method is used in a responsible and ethical manner.

Overall, the proposed method has great potential for further development and research in the field of facial recognition. By addressing the limitations and exploring new avenues of research, the accuracy and applicability of the method can be improved, leading to a wide range of real-world applications.

REFERENCES

[1] B, Pranav & J, Manikandan. (2020). Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks. Procedia Computer Science. 171. 1651-1659. 10.1016/j.procs.2020.04.177.

[2] Nath, Raktim & Kakoty, Kaberi & Bora, Dibya & Welipitiya, Udari. (2021). Face Detection and Recognition Using Machine Learning. 43. 194-197.

[3] Bindushree S, & Rakshitha A N. (2021). Face Recognition Using Deep Learning. International Journal of Advanced Scientific Inovation, 01(01), 12–18. https://doi.org/10.5281/zenodo.4641691

[4] Nadikattu, Arunkumar & P, Kundhan & Sk, John & Panda, Sunita & Chandran, Kamalanathan. (2020). Prevention of Unauthorized Door Access Using Face Recognition Built With Haar Cascade Classifier and Histogram of Oriented Gradients. SSRN Electronic Journal. 10.2139/ssrn.3606883.

[5] Hussain, S. asif & Balushi, Ahlam. (2020). A real time face emotion classification and recognition using deep learning model. Journal of Physics: Conference Series. 1432. 012087. 10.1088/1742-6596/1432/1/012087.

[6] Anwarul, Shahina & Dahiya, Susheela. (2020). A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy. 10.1007/978-3-030-29407-6_36.

[7] Abdulla, Abdulrahman & Abdulraheem, Ahmad & Salih, Azar & M.Sadeeq, Mohammed & Ahmed, Abdulraheem & Ferzor, Barwar & Salih, Omar & Mohammed, Ibrahim. (2020). Internet of Things and Smart Home Security. Technology Reports of Kansai University. 62.

[8] Yedulapuram, Sharvani & Arabelli, Rajeshwarrao & Mahender, K. & Sidhardha, Chintoju. (2020). Automatic Door Lock System by Face Recognition. IOP Conference Series: Materials Science and Engineering. 981. 032036. 10.1088/1757-899X/981/3/032036.

[9] Irjanto, Nourman & Surantha, Nico. (2020). Home Security System with Face Recognition based on Convolutional Neural Network. International Journal of Advanced Computer Science and Applications. 11. 10.14569/IJACSA.2020.0111152.

[10] F. Faisal and S. A. Hossain, "Smart Security System Using Face Recognition on Raspberry Pi," 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Island of Ulkulhas, Maldives, 2019, pp. 1-8, doi: 10.1109/SKIMA47702.2019.8982466.

[11] Pandey, Sachi, Vikas Chouhan, Rajendra Prasad Mahapatra, Devansh Chhettri, and Himanshu Sharma. "Real-time safety and surveillance system using facial recognition mechanism." In Intelligent Computing and Applications: Proceedings of ICICA 2019, pp. 497-506. Springer Singapore, 2021.

[12] M. R. D. Rodavia, O. Bernaldez and M. Ballita, "Web and mobile based facial recognition security system using Eigenfaces algorithm," 2016 IEEE International

Conference on Teaching, Assessment, and Learning for Engineering (TALE), Bangkok, Thailand, 2016, pp. 86-92, doi: 10.1109/TALE.2016.7851776.

[13] Khodadin, Fatimah, and Sameerchand Pudaruth. "An intelligent camera surveillance system with effective notification features." International Journal of Computing and Digital Systems 9, no. 6 (2020): 1251-1261.

[14] Ijaradar, Jyotirmaya, and Jinjing Xu. "A Cost-efficient Real-time Security Surveillance System Based on Facial Recognition Using Raspberry Pi and OpenCV." Current Journal of Applied Science and Technology 41, no. 5 (2022): 1-12.

[15] Bah, Serign Modou; Ming, Fang (2019). An improved face recognition algorithm and its application in attendance management system. Array, (), 100014–. doi:10.1016/j.array.2019.100014.