Intelligent Multicabin Access System Using Face Recognition

Mrs. Reshma
Assistant Professor
Department of CSE
AIT Bengaluru

Shravya U Shetty
Department of CSE
AIT Bengaluru
shravyak.22.becs@acharya.ac.in

Srilakshmi H Y
Department of CSE
AIT Bengaluru
srilakshmiy.22.becs@acharya.ac.in

Suvarna
Department of CSE
AIT Bengaluru
suvarnaa.22.becs@acharya.ac.in

***Abstract*—Because keys can be misplaced, copied without permission, or fail to offer flexible control over access rights, conventional key-based locking systems frequently result in everyday inconvenience and security issues. This project offers an intelligent multi-chamber access control system that combines facial recognition with straightforward remote management to get around these restrictions. The primary controller for several chambers is a single Raspberry Pi, which uses LBPH for quick and accurate recognition even on low-power hardware and Haar Cascade for face detection. The system automatically unlocks the designated chamber when an authorized person approaches. The system takes a picture and immediately notifies the chamber owner via Telegram if it detects an unidentified face, enabling real-time access approval or denial.Owners can also use basic bot commands to remotely lock or unlock their chambers. This system is appropriate for offices, research labs, and other settings that need controlled multi-user access because it offers better security, easier administration, and increased flexibility.**

***Keywords*—Telegram Bot, LBPH, Haar Cascade, Raspberry Pi, IoT Security, Face Recognition, Access Control System, Multi-Chamber Locking, Remote Authentication, Embedded Systems, Smart Locking System.**

I. INTRODUCTION

Modern environments have much higher security requirements than what conventional mechanical locks can consistently provide. Physical keys offer very little control once they are out of the owner's possession, are easily lost, and can be copied without authorization. There is a noticeable trend toward intelligent and automated access control systems as shared spaces and workplaces require safer and more practical ways to control entry.

With the quick development of artificial intelligence and embedded computing, facial recognition has emerged as one of the most useful techniques for secure and contactless identity verification. These systems can quickly and easily authenticate users by examining distinctive facial features. Integrating automated hardware elements like solenoid locks and relays makes the process much more reliable and efficient overall, guaranteeing that only those who have been verified are granted access.

The Intelligent Multi-Cabin Access System bridges traditional locking mechanisms with intelligent automation in order to meet these contemporary expectations. In addition to a camera module, display, and electronic locking units, the system uses a Raspberry Pi as the central controller to manage several cabins in a single configuration. Every cabin has a unique user assigned to it, and entry is only possible after facial recognition is successful. When the system detects an unfamiliar face, it immediately takes a picture and sends a Telegram bot to the relevant cabin owner, who can then approve or reject the access attempt from any location.

Because of this strategy, the system is especially well-suited for places where security and accountability are essential, such as offices, labs, coworking spaces, and storage facilities. Owners can lock or unlock their cabins from a distance using remote control tools and real-time notifications. The system provides a flexible, scalable, and secure access control solution for contemporary multi-user situations by fusing automated hardware, IoT-based communication, and facial recognition.

II. LITERATURE SURVEY

Numerous methods are being researched for face-recognition-based access systems with the goal of enhancing real-time performance, accuracy, and robustness. In one line of work, the Viola-Jones detection method is combined with HOG features, followed by CNN-based classification and binary code generation based on reinforcement learning. Even in a variety of environmental circumstances, this integrated approach reports an accuracy of 98.85% [1]. Another noteworthy technique tracks facial features using the KLT algorithm and employs Haar Cascade for detection. Euclidean-distance matching and eigenfaces derived from PCA are then used to verify identity [2]. Additionally, improvements to HOG preprocessing have been investigated, especially in hybrid CNN-KELM models that achieve strong performance with very few training epochs by reducing feature dimensions and fine-tuning Gaussian kernels using grid search [3].Several studies investigate broader machine-learning frameworks for facial recognition, employing supervised techniques such as CNNs and discriminant analysis, as well as unsupervised clustering models like k-means and DBSCAN. These systems frequently rely on PCA, LDA, and optimizers including Adam and SGD to boost classification reliability [4]. Deep-learning-driven solutions, such as CNNs and Siamese architectures,

have shown high precision by extracting key facial landmarks and applying metrics such as Euclidean distance or triplet-loss-based embedding comparison. Many of these models adopt MTCNN for alignment and Inception-ResNet V1 for generating compact embeddings [5]. A related set of approaches combines MTCNN with FaceNet to produce 128-dimensional representations, enabling stable verification despite changes in facial pose or lighting [6].Further contributing to effective feature extraction appropriate for real-time execution on embedded devices are lightweight networks such as MobileNetV2 [7]. Other implementations achieve frame rates between 30 and 60 FPS by combining ArcFace's angular-margin-based classification with YOLOv5 for high-speed face detection [8]. For low-resource environments that require little training data, traditional combinations like PCA and LDA combined with SVM or RBF classifiers continue to provide efficient solutions [9]. Before classification using Chi-square comparison metrics, LBPH enhanced with CLAHE pre-processing improves illumination quality in low light [10].To achieve high accuracy with fewer parameters, more sophisticated topologies like EfficientNet-B3 use compound scaling, Swish activation, and RMSProp optimization [11]. By considering images as sequences of patches and employing multi-head attention to collect long-range characteristics, Vision Transformers (ViT) offer a different approach that helps them deal with occlusions and lighting fluctuations [12]. By combining multimodal data prior to classification, dual-stream CNNs—which analyze both thermal and visual images—offer better recognition performance in low-visibility or dark environments [13].By comparing embedding distances rather than retraining the entire model, one-shot learning with Siamese networks and contrastive loss allows for quick onboarding of new users [14]. Lastly, by producing frontal facial reconstructions prior to verification, 3D Morphable Models (3DMM) aid in standardizing position and lighting and enhance accuracy when the camera records faces from difficult angles [15].

III. RESEARCH GAPS

Many of the current systems are made to work on a single door or for a single user, despite the fact that facial recognition has emerged as a dependable and popular technique for safe authentication. They are therefore inappropriate for real-world settings where multiple cabins or compartments must be controlled simultaneously. Furthermore, many existing solutions rely significantly on expensive hardware or cloud-based processing, which restricts their applicability in real-time applications on reasonably priced embedded devices like the Raspberry Pi. As a result, a number of systems are unable to provide useful performance in situations that call for rapid processing and inexpensive deployment.

The absence of integrated functionality for remote verification, alerting, or decision-making is another disadvantage of the majority of facial recognition-based locking systems. When an unidentified individual shows up, these systems usually only prevent entrance without offering the cabin owner a way to verify the user's identity or allow entry from a distance. Their efficacy is diminished by the lack of remote engagement, particularly in shared or distributed settings where quick reactions and adaptable control are crucial.Additionally, traditional biometric systems do not allow individualized access control for each user or centralized monitoring of several chambers. The majority of current methods prevent unidentifiable people from entering without providing a way for remote permission, override, or further confirmation. In contemporary organizations, where numerous users require accountable and controlled access, this gap is crucial. A system that combines lightweight, effective facial recognition with automated locking hardware and Internet of Things-based remote communication is needed to overcome these constraints and provide a safe, scalable, and useful solution for multicabin setups.

IV. OVERVIEW OF THE PROPOSED SYSTEM

By offering a clever and automated mechanism for handling several cabins, the suggested system seeks to get beyond the drawbacks of conventional key-based access techniques. Conventional locks frequently result in issues like missing keys, illegal duplication, and trouble controlling access when numerous individuals are involved. In order to address these problems, the system employs facial authentication, using the LBPH algorithm for recognition and Haar Cascade for face detection. This allows for rapid and safe access without the need for physical keys.

The central controller is a Raspberry Pi that interfaces with an LCD display, camera, solenoid lock, relay module, and buzzer. The technology detects and verifies a person's face in real time when they stand in front of it. The matching cabin unlocks automatically if the person is identified as an authorized user. If the system sees an unknown person, it quickly takes the image and communicates it to the cabin owner using Telegram, letting them to determine whether access should be permitted.

The system is perfect for office cabins, labs, co-working spaces, and safe storage units due to its modular and structured architecture. Owners may control access from any location thanks to the system's remote verification feature, which makes it both practical and extremely safe. The solution provides a scalable and dependable substitute for conventional access control systems by combining facial recognition, embedded hardware, and Internet of Things connectivity.

V. SYSTEM ARCHITECTURE

The Intelligent Multi-Chamber Access System's architecture combines hardware and software elements, each of which has a distinct function to guarantee safe and automated access control.

A. Core Processing Unit

The Raspberry Pi serves as the setup's primary decision-making component. It:

- receives the live video frames that the camera has recorded
- uses the Haar Cascade classifier to recognize faces
- uses the LBPH algorithm to carry out recognition
- decides whether to grant access or unlock the system

B. Camera Module

Every person in front of the system is continuously photographed by the camera. After that, the Raspberry Pi receives these frames and uses them for detection and verification.

C. Locking Mechanism

- The Raspberry Pi and the hardware lock are interfaced by the relay module
- When a user is verified, the solenoid lock opens on its own
- The locking mechanism is still in place for security in the event that authentication is unsuccessful

D. Security Components

- When someone tries to gain unauthorized access, a buzzer sounds an alert
- Real-time system messages like "Access Granted," "Access Denied," and "Face Not Detected" are shown on the LCD panel

E. Telegram Remote Interface

During an unidentified user's attempt:

- The apparatus takes a picture
- uses Telegram to send it straight to the cabin owner
- Access can be remotely verified, approved, or denied by the owner

F. Software Framework

Before being sent to the identification module, OpenCV is utilized to preprocess photos and transform frames from BGR to RGB, guaranteeing correct image handling and precise analysis.

VI. Modules Description

The system is divided into a number of useful modules, all of which support intelligent and smooth access control. When combined, these modules provide precise identification, safe functioning, and efficient remote monitoring.

A. User Authentication Module

This module is in charge of:

- Using the Haar Cascade classifier to identify faces
- Using the LBPH algorithm to identify users
- Comparing the stored training dataset with real-time face input

B. Image Capture and Unauthorized Logging Module

- Taking pictures of users who don't pass authentication
- Keeping these documents for audits and future reference
- Using Telegram to send the taken pictures to the cabin owner for confirmation

C. Access Control Module

- Relay and solenoid lock activation upon user verification
- Unlocking the designated cabin automatically for those who are permitted
- If authentication fails, all cabins should be kept safely locked

D. Notification and Alert Module

- Notifying owners instantly via Telegram
- Setting off buzzer alerts when illegal attempts occur
- Notifying owners of all significant system occurrences

E. Display and User Interface Module

- "Door Opened"
- "Access Refused"
- "Face Not Found"

F. Database and Storage Module

- Training databases of facial images
- Model files trained with LBPH
- Access attempt logs and pictures of unidentified users

VII. RESULTS

The accuracy and stability of the Intelligent Multi-Chamber Access Control System were assessed under a variety of real-world scenarios. The LBPH algorithm for recognition and Haar Cascade for face detection provided reliable results, guaranteeing that only those with permission were allowed access. In order to facilitate rapid and remote verification, the system immediately took a picture of any unfamiliar people attempting to enter a cabin and sent it to the owner via Telegram.

The Raspberry Pi, camera module, solenoid lock, relay, buzzer, and other hardware parts all synchronized with the software modules to produce seamless and continuous operation. Under various lighting conditions, face angles, and distances, the system remained accurate in its recognition. The prompt delivery of Telegram alerts greatly enhanced user convenience and overall system usage. These findings attest to the suggested system's dependability, security, and suitability for multi-cabin settings including offices, labs, and shared workplaces.

The system's resilience was further tested under various user and environmental circumstances. It reliably recognized authorized users, identified faces, and blocked access to unidentified people. Unauthorized users' images were appropriately taken, stored, and shared via Telegram with the cabin owner. During real-time operations, every hardware component reacted appropriately, strengthening the system's dependability. The system's performance, hardware interactions, and reaction behavior under various testing scenarios are depicted in the accompanying figures.

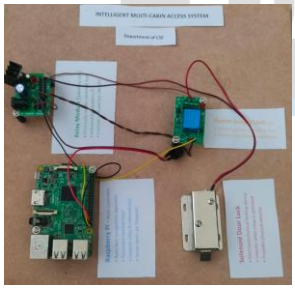

Fig. 1: Hardware configuration for the multi-chamber access control system.

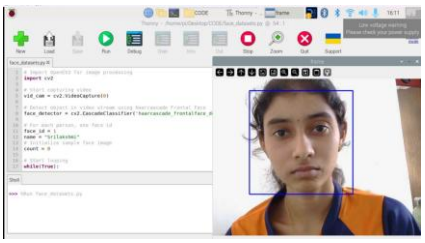

Fig. 2: Face recognition with the Haar Cascade classifier.

Fig. 3: Facial recognition training dataset development procedure.

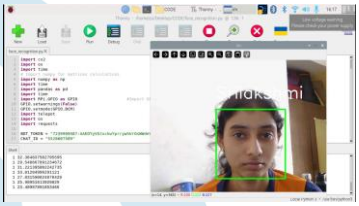

Fig. 4: Real-time LBPH-based face recognition.

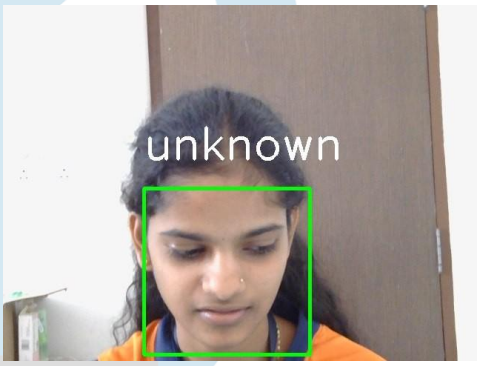

Fig. 5: A picture taken of an unidentified or unauthorized user .

Fig. 6: The cabin owner received a Telegram notification with the taken image .

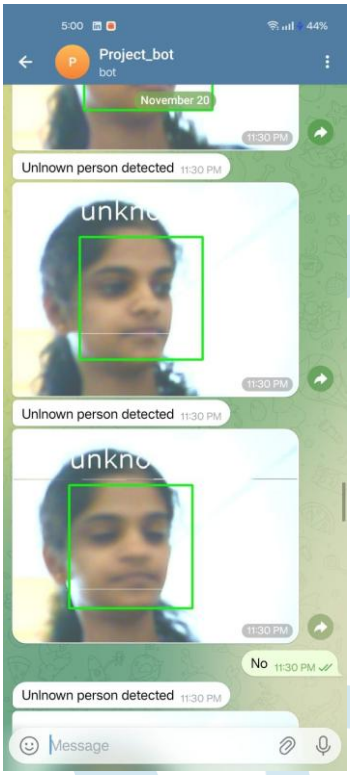

Fig. 7: Owner confirming and answering the Telegram access request.

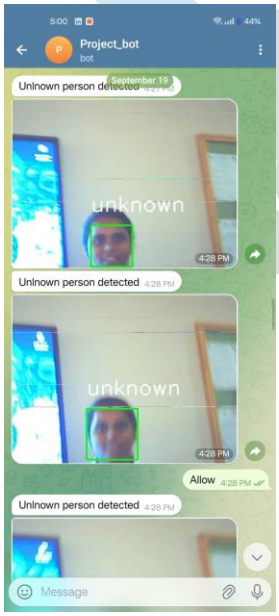

Fig. 8: Telegram commands are used to remotely lock and release the cabin.

The above figures present the system's real-time performance, the interaction among its hardware components, and the response of the proposed intelligent multi-chamber access system under different testing conditions.

VIII. Technologies and Tools Used

A. Software Technologies

1) Python: Python was chosen due to its straightforward syntax, extensive library support, and excellent interoperability with hardware interfaces and computer vision tasks.

2) OpenCV: Face detection, image preprocessing, and the extraction of crucial visual elements needed for recognition are all done with this library.

3) Haar Cascade Classifier: Because of its quick detection speed and low processing cost, the Haar Cascade approach is favored for Raspberry Pi-based applications.

4) LBPH Algorithm: LBPH is used for facial recognition because it works well on low-resource devices, performs accurately even in different lighting conditions, and frequently outperforms traditional techniques like PCA, LDA, and some CNN models on Raspberry Pi.

B. Hardware Technologies

1) Raspberry Pi: Because it can run a full operating system, do demanding image processing tasks, and offer a variety of hardware interface options, the Raspberry Pi functions as the primary controller.

2) Raspberry Pi Camera Module: This module is preferred over conventional USB cameras due to its low latency, excellent real-time capture, and superior integration with the Raspberry Pi.

3) Solenoid Lock and Relay Module: The relay guarantees safe switching and control of the locking mechanism, while the solenoid lock provides dependable electromagnetic locking.

4) LCD Display and Buzzer: To improve security and user interaction, the LCD displays visual feedback while the system is operating, and the buzzer sounds a warning.

5) Telegram Bot API: Telegram is used for secure communication, cloud-based messaging, handling multimedia, and the added advantage of not requiring a dedicated server.

IX. Advantages of the Proposed System

Compared to conventional key-based locking techniques, the suggested access control system has a number of significant advantages. Common dangers associated with physical keys are eliminated, including loss, duplication, and illegal handling. The method offers fast and precise identity

verification in a variety of lighting conditions by utilizing facial authentication via Haar Cascade and LBPH.

The configuration allows for accurate and centralized control from a single unit as the Raspberry Pi is in charge of several chambers. Cabin owners can authorize or reject access without being physically present thanks to the incorporation of Telegram-based remote verification, which significantly increases convenience.

By taking pictures of attackers, giving real-time alerts, and sounding buzzer warnings during questionable efforts, the technology further improves security. Because of its modular design, it may easily be expanded to accommodate additional cabins or users as needed. These features make the system ideal for shared workstations, offices, labs, and storage settings. All things considered, it combines IoT communication, automation, and intelligent identification to provide a safe and easy-to-use access management system.

X. Conclusion and Future Scope

A. Conclusion

The project effectively displays an intelligent multi-cabin access control system that integrates automatic authentication, facial detection, and identification. Even in small-scale deployments, the system guarantees accurate and reliable access management by using Haar Cascade for real-time face detection and LBPH for face recognition. Verified users can easily obtain access without physical keys, while unauthorized attempts are instantly prevented.

By integrating a Telegram bot, security and control can be improved through remote monitoring, immediate notifications, and the preservation of photos of unidentified people. The Raspberry Pi, camera, solenoid lock, relay, buzzer, and other hardware parts cooperate to provide dependable and seamless operation. The system's accuracy, stability, and real-time response were validated by tests conducted in various lighting conditions, angles, and surroundings. All things considered, this system combines effectiveness and user convenience to offer a contactless, hygienic, and safe access solution.

B. Future Scope

1) Improvements to Functional and Non-Functional Elements:

- incorporating cutting-edge deep learning models to improve recognition accuracy, such as FaceNet or MobileFaceNet.
- To stop spoofing, liveness detection (such as blink detection, IR sensors, or 3D depth cameras) should be added.
- AI hardware, such as Coral TPU or Jetson Nano, can speed up processing.
- application of multi-factor authentication that combines fingerprint scanning, RFID, or facial recognition with OTPs.
- All conversations should be fully encrypted to protect important information.
- creation of an online dashboard for user management, monitoring, and access log analysis.
  -based backup to protect data, including logs, datasets, and taken pictures.

2) Expansion and Broader Application Scope:

- expanding the system to accommodate multi-cabin buildings, offices, labs, warehouses, hostels, and apartments.
- IoT device integration for alarm automation, lighting, and surveillance.
- development of a mobile application for monitoring, notifications, and real-time control.
- temporary QR codes or time-limited access for visitor management.
- Analytics for creating usage data, monitoring access trends, and identifying irregularities.
- Geo-fencing features that automatically unlock when authorized users get close.
- Battery backup and offline operation to guarantee continuous functioning.

References

[1] A. Kumar, R. K. Yadav, and D. K. J. B. Saini, "A new method for robust video face recognition using convolutional neural networks," *ePrime - Advances in Electrical Engineering, Electronics and Energy*, vol. 5, pp. 100241–100361, 2023.

[2] A. J. and P. Suresh, "A novel fast hybrid face recognition approach using convolutional kernel extreme learning machine with HOG features," *Measurement: Sensors*, vol. 30, pp. 100907–100915, 2023.

[3] C. R. Kumar, S. N. Saranya, M. Priyadharshini, D. G. E. Derrick, and K. R. M. Kaleel, "Face recognition using CNN and Siamese network," *Measurement: Sensors*, vol. 27, pp. 100800–100835, 2023.

[4] S. D. Lin and P. E. Linares Otoya, "Pose-invariant face recognition using facial landmark based ensemble learning," *IEEE Access*, vol. 11, pp. 44221–44233, 2023.

[5] H.-T. Ho, L. V. Nguyen, T. H. T. Le, and O.-J. Lee, "Face detection using eigenfaces: A comprehensive review," *IEEE Access*, vol. 12, pp. 118406–118422, 2024.

[6] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE CVPR*, pp. 815–823, 2015.

[7] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "MobileNetV2: Inverted residuals and linear bottlenecks," in *Proc. IEEE CVPR*, pp. 4510–4520, 2018.

[8] J. Deng et al., "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. IEEE/CVF CVPR*, pp. 4690–4699, 2019.

[9] W. Zhao, R. Chellappa, and P. J. Phillips, "Subspace linear discriminant analysis for face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–570, 2007.

[10] T. Ahonen, A. Hadid, and M. Pietika¨inen, "Face recognition with local binary patterns," in *European Conference on Computer Vision (ECCV)*, pp. 469–481, 2004.

[11] M. Tan and Q. V. Le, "EfficientNet: Rethinking model scaling for convolutional neural networks," in *Proc. ICML*, pp. 6105–6114, 2019.

[12] A. Dosovitskiy et al., "An image is worth 16x16 words: Transformers for image recognition at scale," in *Proc. ICLR*, 2021.

[13] Z. Zhu et al., "A thermal-visible face recognition system based on stream CNN," *IEEE Sensors Journal*, vol. 22, no. 5, pp. 3981–3992, 2022.

[14] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition using CNNs," in *BMVC*, 2015.

[15] Z. Liu et al., ”SphereFace: Deep hypersphere embeddings for facial recognition,” in *Proc. IEEE CVPR*, pp. 212–220, 2017.
[16] Y. Wu, H. Liu, J. He, and Y. Fu, ”LightCNN: Lightweight deep networks for face representation,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 3048–3058, 2018.
[17] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, ”VGGFace2: Dataset for face recognition across pose and age,” in *Int. Conf. Automatic Face and Gesture Recognition (FG)*, pp. 67–74, 2018.
[18] J. Wang, Y. Luo, and Z. Hu, ”Cross-spectral face recognition using deep perceptual mapping,” *IEEE Transactions on Multimedia*, vol. 21, no. 11, pp. 2873–2883, 2019.
[19] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, ”ArcFace: Additive angular margin loss for deep face recognition,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 42, no. 10, pp. 2251–2263, 2020.
[20] K. He, X. Zhang, S. Ren, and J. Sun, ”Deep residual learning for image recognition,” in *Proc. IEEE CVPR*, pp. 770–778, 2016.
[21] F. Schroff, D. Kalenichenko, and J. Philbin, ”FaceNet: A unified embedding for face recognition and clustering,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 2, pp. 212–229, 2014.
[22] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, ”Labeled Faces in the Wild: A database for studying face recognition in unconstrained environments,” *Technical Report 07-49, University of Massachusetts, Amherst*, 2007.
[23] J. Taigman, M. Yang, M. Ranzato, and L. Wolf, ”DeepFace: Closing the gap to human-level performance in face verification,” in *Proc. IEEE CVPR*, pp. 1701–1708, 2014.
[24] A. Kumar, R. K. Yadav, and D. K. J. B. Saini, ”Face recognition using deep learning: A survey,” *International Journal of Computer Vision and Image Processing*, vol. 8, no. 2, pp. 45–60, 2022.
[25] S. Zafeiriou, C. Zhang, and Z. Zhang, ”A survey on face detection in the wild: Past, present and future,” *Computer Vision and Image Understanding*, vol. 138, pp. 1–24, 2015.