Design of Face Recognition Security System on Public Spaces

1st F. M. Dirgantara
Computer Engineering
Telkom University
Bandung, Indonesia
fussymentari@telkomuniversity.ac.id

2nd D.P. Wicaksa
Electrical Engineering
Bandung Institute of Technology
Bandung, Indonesia
dpwicaksa@students.itb.ac.id

***Abstract*— Implementation of physical security such as recruitment of security officers, installation of CCTV, and restrictions on public access have become commonplace nowadays. Computer systems equipped with archival storage media must be properly maintained, including computer systems containing sensitive information that must be stored in a locked and secure place. This study applies a security system using facial recognition to determine who is authorized over the data in the computer system—using Haar Cascade as a face detector and LBPH as a match between faces that can access and those that are not on the list. On the other hand, if the person is unidentified, preventive measures will be performed. Based on the result, the proposed system using Raspberry Pi 4 is able to identify a face using Haar Cascade algorithm with an accuracy of 68% and average duration process of 0.392s, and able to recognize face using LBPH algorithm with accuracy between 50.74% to 100% and average duration process of 0.548s.**

Keywords*— *security system face detection, Haar Cascade, face recognition, LBPH

I. INTRODUCTION

The aspect of security is intangible. If a system's security is insufficient, it can have various negative impacts [1], including physical security [2], such as the security of a room that unauthorized persons can access [3]. Conventional techniques of physical security, for example a locking mechanism, are still used for the majority of physical security [4]. If unauthorized people are able to gain access through other gaps, it will be ineffectual [5]. Theft and other crimes in the business frequently occur while the situation is quiet and the owner or security officials are not present. As a result, the security system's vulnerability remains high [6].

Implementation of physical security measures such as hiring security guards, installing closed-circuit television [7], and restricting public access are quite common nowadays. Computer systems, storage media, and backups must all be limited and safeguarded. Computer systems containing sensitive information are kept in locked and secure areas. Technically, access restrictions such as passwords or directory access rights are required to strengthen the security process [8][9]. Threats to data centers, data processing facilities, and staff will be prevented by combining physical security with specified functionality [10] [11].

State of the art about this security systems research are smart home utilizing face recognition system [12] by Wati et al. The system is tested using MyRIO 1900 to see how well it detects faces based on changes in distance and the person's accessories, which aren't all recognized. Another example is security system for bank adopting biometric authentication in ATM [13] by Gusain et al. Face identification was achieved utilizing a canny edge detector in this study, which combined face detection and recognition. One of the recent research for security system using camera at the airport by Zhu et al. [14] for verification process. Security checkpoint are including camera for face recognition in need for self-service centralized verification and automatic face recheck for passenger.

As a solution, a security system prototype was created, which uses a microcomputer as the physical security system's brain [15]. When the panel is open, the microcomputer will detect it and signal that the panel has been accessed by an unauthorized individual. An alarm that signals when unauthorized individuals access the area or if there are changes in the system's true state according to the readings but without the presence of an authorized individual can be indicators of a physical security attack. Another indicator is camera footage, which demonstrates that there are persons who do not have the right to be caught on camera. Damage to the panel lock, evidence such as the presence of foreign objects around the panel, loss of communication signal, or the device being lost or disappearing without being recorded/no one knowing where it is, are all possibilities. When it is determined that someone unauthorized is accessing the system physically, a warning along with camera feed from the panel will be issued to officer-in-duty as a preventive measure. Therefore, it is hoped that the officers will be able to take the appropriate measures against the criminals right away.

The main goal of this research is to help industries supervise and regulate the security panel from their control area and cellphone. Mobile devices, such as smartphones, can access and control the system via a user-friendly interface from anywhere and anytime [16]. Supervision is the study of a person's behavior, exercise, or knowledge of how information develops and how it can be used to influence, monitor, regulate, or secure [17]. We may use this system to not only supervise and regulate, but also to perform actions like alarm activation and door lock control. The system emits an alarm sound according to the command message [18]. When the system receives a control message from the user to lock the door, the panel will be locked. The security system becomes better and easier as a result of these actions, because the smartphone can be conveniently used as a control panel [19].

This topic has been the subject of numerous researches. A control panel with an application feature system in the form of door control, video streaming, and image capture are used in one of the experiments [20]. In this study, a data logger was prepared to provide information on activities that occur around the train panels. The physical security system will collect photographs of perpetrators who gain access to the panel without permission. If the panel is closed, the

system will immediately enter a locked state; if the panel is opened, the locking system will record and notify the working officer of the acquired image.

II. METHODS

A. System Design

Fig. 1 depicts a system overview that describes the stages of the face recognition process from start to finish. The system's stages of operation are listed below.

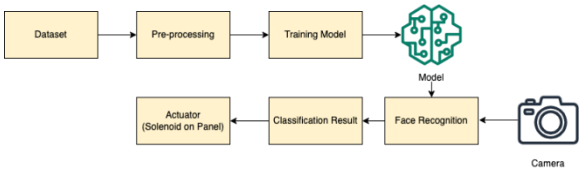

Fig. 1. Design of face recognition security system on public places

The unprocessed dataset is converted to a matrix-form of a grayscale image during pre-processing. Then after the training process, an actual model based on the training model is produced using Local Binary Patterns Histogram (LBPH) algorithm. Face recognition algorithms such as Sparse Coding (SC), Local Binary Pattern (LBP) method, Histograms of Oriented Gradients (HOG) algorithm, and others have been developed. While existing algorithms have accuracy rates of 50 to 60 percent, the LBPH algorithm is capable of recognizing not only the front face, but also the side face with a rate of more than 90 percent [21]. The LBP and HOG descriptors are merged in the LBPH method. LBP is a simple yet effective method for extracting and labeling pixels in an image. As a result, the LBPH technique can be used to represent facial images using a simplified vector [22]. The model is used to detect if a face is present in the images from the camera and if it is present, the system will try to recognize the detected face. On the camera frame window that displays the camera feed, the classification results will be displayed in real time. Based on the classification result, the system will issue commands to move the solenoid to open or close the lock as illustrated in Fig. 2.

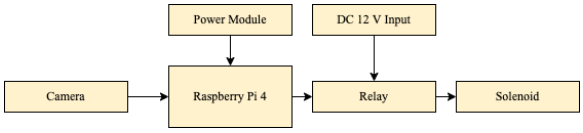

Fig. 2. Security panel on public places block diagram

The Raspberry Pi 4 serves as the brain of the system, to process data and control the overall operation. Images from the camera are processed by the system and compared with data in the database to see if the face matches the one in the database. The relay acts as a driver for the solenoid switch, allowing electric current to enter the solenoid to be turned on or off. The solenoid in this system is responsible for locking or unlocking the panel door. The solenoid is controlled by the relay's output according to the processor's decision.

The system implementation is shown in Fig. 3. In the initial phase, the system will load a database containing a descriptor for face and specific face to be recognized. In the whole process, there are two major image processing stages. First, the system will try to detect the presence of a face in the image. If a face is detected, then it will crop the image based on the region of interest and use it on the next image processing stage. In the next stage, the face feature is extracted and it will be compared with saved data in the database. If the feature matches one of the saved faces in the database, then the system will acknowledge the person and issue commands to unlock the door. On the other hand, if the face is not recognized, it will be saved in a data logger and the door remains locked.

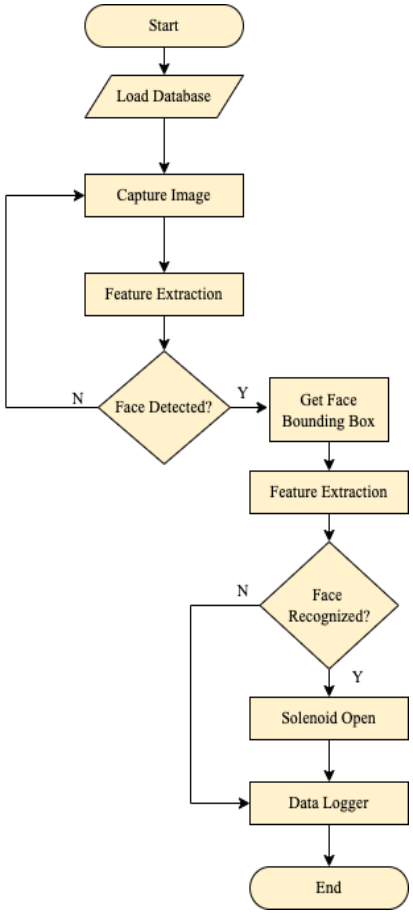

Fig. 3. Face recognition security system flowchart

B. Implementation

The locking system is implemented in hardware in this system. This system is designed to be as basic and feasible as possible while still providing maximum efficiency. This system's hardware implementation does not necessitate a big number of tools or hardware; it only requires a camera, processor, and actuator. Fig. 4 represents the illustration and the actual components that are used in the prototype.

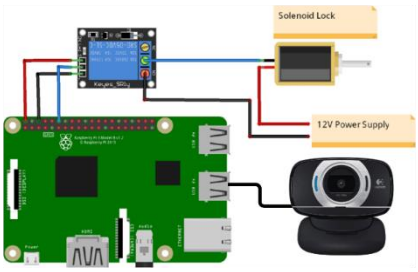

Fig. 4. Prototype design

Raspberry Pi 4 is chosen as a processor in the prototype. It has USB ports that can be used for webcam or external input devices for debugging purposes such as keyboard and mouse, display port to show the camera feed and image processing results, GPIO to control the actuator, and ARM v8 processor and 8GB RAM to support calculation of image processing.

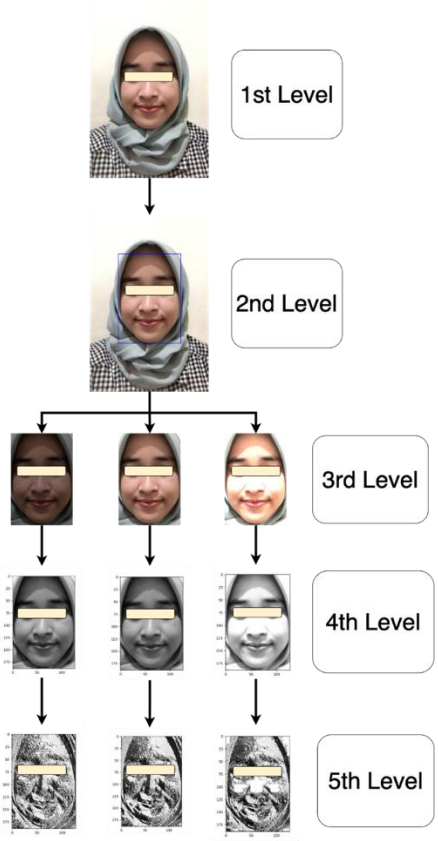

Fig. 5. Steps of image processing

Fig. 5 show the image processing in the proposed system. The Haar Cascade algorithm is used to identify presence of a face despite differences in illumination, scale, pose, and camera variation [23] [24]. The result of Haar Cascade algorithm is depicted in the second level to identify area that contains a face. To be able to recognize a face, the system requires a dataset of the person's face. In this study, we use 250 images per person facing a camera from various angles to make the dataset. The third and fourth level depicted images that have been cropped and normalized according to the region of interest produced by Haar Cascade algorithm.

Face is able to provide non-intrusive identification. The fifth level of image processing is an LBP images. Despite of differences in lightning between images in fourth level, the LBP images able to produce almost similar images. To incorporate spatial information in LBP model, it is divided into several local region and a histogram will be extracted from each region. The spatially enhanced feature vector is then obtained by concatenating the local histograms. Each face is given specific ID and name for logging purpose. For registration, the training subject is asked to face the camera and move her/his face at different angles for 10 second to make an initial training dataset.

III. Results and Discussion

In this experiment, 12 person participates as a model and only half of them is registered in the database. Haar Cascade algorithm is used to detect presence of a face and LBPH algorithm is used to recognize the face and the final conclusion is taken based on the confidence level. The results are as follows.

A. Face Detection using Haar Cascade

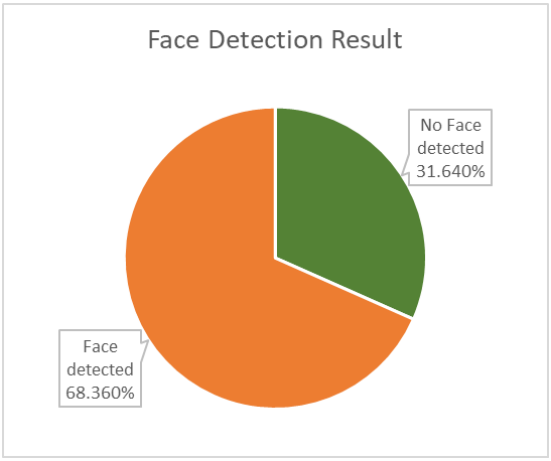

Fig. 6. Haar Cascade face detection result

Fig. 6 show the result of face detection using Haar Cascade algorithm. Video files are used for testing with an average duration of 20s in each video. By capturing the video feed, a frame is acquired. The system is able to detect presence of a face in 68.360% of samples. Based on observation during the test, the system is more capable to detect presence of a face if the face is facing the camera and not moving too fast. Fig. 7 shows occurrences where the system fails to detect presence of a face. The failure to detect presence of a face can be caused by face angles that hidden the face feature, as shown in 7a and 7c. 7b is most likely happen because of the addition of hat and hand gesture that interfere with the face.

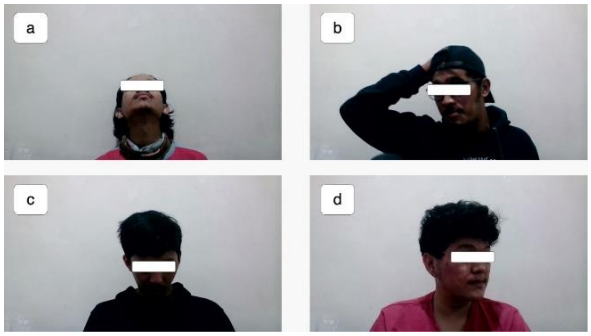

Fig. 7. Sample of undetected faces

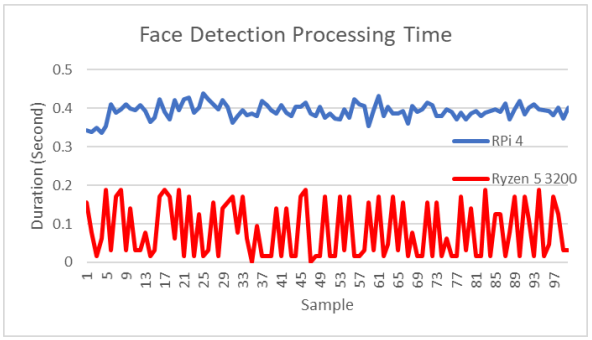

Fig. 8. Haar Cascade processing time

Fig. 8 shows processing time required to perform a face detection. Face detection process is done with an average duration of 0.392s, a 0.439s maximum duration, and a 0.337s minimum duration. To make a comparison, same program is executed in a computer with Ryzen 5 3200 processor and 16GB RAM. The result is the program is done with an average duration of 0.082s, a 0.187s maximum duration, and 0.015s minimum duration.

B. Face Recognition using LBPH

Fig. 9. Sample of recognized faces

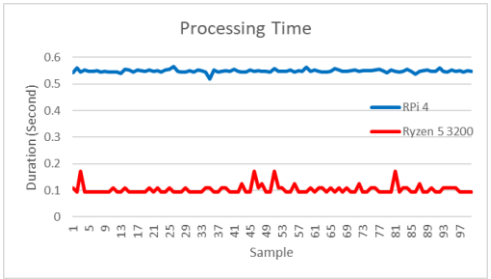

Fig. 10. LBPH processing time

Fig. 9 shows occurrences when the system is able to recognize and differentiate faces. In the display, confidence level along with preregistered ID will be shown around the face bounding box. In Raspberry pi 4, face detection process using LBPH algorithm is done with an average duration of 0.548s, a maximum 0.566s duration, and a 0.518 minimum duration. On a Ryzen 5 processor, the LBPH algorithm is done with an average duration of 0.102s, a 0.171s maximum duration, and a 0.093s minimum duration as shown in Fig. 10.

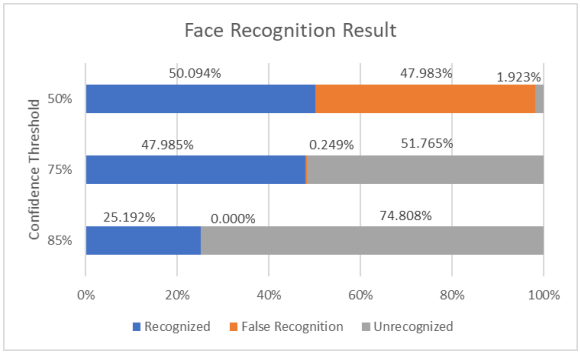

Fig. 11. LBPH face recognition result

The face recognition result is based on the confidence threshold to make a conclusion. It means that if the confidence level of a recognition process is above the threshold, then the system will acknowledge it as recognized. A ‘false positive’ flag means the system determines that the face is existed in the database, but in reality, the face is not registered. An example of false positive occurrence is when an unknown person is recognized by the system as someone that already registered in the database instead of flagged as an ‘unrecognized’. An ‘unrecognized’ flag means that the system determines the face sample is not exist in the database.

As shown in Fig. 11, by using 50% confidence threshold, 50.094% face samples are flagged as ‘recognized’, 47.983% face samples are flagged as a 'false positive’, and 1.923% face samples are flagged as ‘unrecognized’. By increasing the confidence threshold into 75%, it reduces the ‘false positive’ flag to 0.249%, the ‘recognized’ flag to 47.985% and an increase in ‘unrecognized’ flag to 51.765%. By further increasing the confidence threshold to 85%, 25.192% faces are ‘recognized’ and 74.808% faces are ‘unrecognized’ with a 0% face detected as a false positive.

By increasing the confidence threshold, a false positive can be eliminated. However, it will take longer for a registered person to be recognized because of the high threshold. Based on the result in 85% confidence threshold, it can be said that for every 4 face samples acquired by the system, 3 of them are flagged as unrecognized and the other one can be correctly recognized. The recognized sample accuracy is quite high compared with results from using 50% confidence threshold, where from every 2 images 1 of them can be recognized correctly while the other one will be recognized as another registered person.

.

IV. Conclusion

Following the results of the experiments, it can be determined that the proposed system has met the research's objectives. The Haar feature is used in this system's to detect presence and recognize a face in an images. This method can classify a variety of facial photos. The system will either lock or unlock the door through solenoid according to the recognition result. The system able to keep track of the known and unknown users who have used it. Faces that are not recognized by the system are saved as photographs in the local directory. According to the results, the proposed system using the Raspberry Pi 4 can identify a face using the Haar Cascade algorithm with a 68 percent accuracy and a 0.392s average process time, and recognize a face using the LBPH algorithm with a 50.74 percent to 100 percent accuracy and a 0.548s average process time.

Acknowledgments

Thanks to PPM Telkom University for supporting this journal's publication process through the Internal Research Grant.

References

[1] S. K. Choi, C. H. Yang, and J. Kwak, "System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats," KSII Transactions on Internet and Information Systems (TIIS), vol. 12, no. 2, pp. 906-918, Feb. 2018, doi: 10.3837/TIIS.2018.02.022.

[2] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-Learning-Enabled Security Issues in the Internet of Things," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9531-9538, Jun. 2021, doi: 10.1109/JIOT.2020.3007130.

[3] R. H. Sloan and R. Warner, Unauthorized Access: The Crisis in Online Privacy and Security. Taylor & Francis, 2017.

[4] Z. Lv, D. Chen, R. Lou, and H. Song, "Industrial Security Solution for Virtual Reality," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6273-6281, Apr. 2021, doi: 10.1109/JIOT.2020.3004469.

[5] S. Kumar, S. Swetha, V. T. Kiran, and P. Johri, "IoT based smart home surveillance and automation," 2018 International Conference on Computing, Power and Communication Technologies, GUCON 2018, pp. 786-790, Mar. 2019, doi: 10.1109/GUCON.2018.8674999.

[6] N. A. Hussein and I. al Mansoori, "Smart Door System for Home Security Using Raspberry pi3," 2017 International Conference on Computer and Applications, ICCA 2017, pp. 395-399, Oct. 2017, doi: 10.1109/COMAPP.2017.8079785.

[7] T. Sikandar and K. H. Ghazali, "A Review on Human Motion Detection Techniques for ATM-CCTV Surveillance System," International Journal of Computing, Communication and Instrumentation Engineering, vol. 3, no. 2, May 2016, doi: 10.15242/IJCCIE.IAE0516006.

[8] A. R. Syafeeza et al., "IoT based facial recognition door access control home security system using raspberry pi," International Journal of Power Electronics and Drive System (IJPEDS), vol. 11, no. 1, pp. 417-424, 2020, doi: 10.11591/ijpeds.v11.i1.pp417-424.

[9] M. Mathew and R. S. Divya, "Super secure door lock system for critical zones," in 2017 International Conference on Networks and Advances in Computational Technologies, NetACT 2017, Oct. 2017, pp. 242-245. doi: 10.1109/NETACT.2017.8076773.

[10] B. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," Sensors 2018, Vol. 18, Page 817, vol. 18, no. 3, p. 817, Mar. 2018, doi: 10.3390/S18030817.

[11] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," Future Internet 2019, Vol. 11, Page 89, vol. 11, no. 4, p. 89, Apr. 2019, doi: 10.3390/FI11040089.

[12] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," in Proceedings - 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2017, Feb. 2018, vol. 2018-January, pp. 342-347. doi: 10.1109/ICITISEE.2017.8285524.

[13] R. Gusain, H. Jain, and S. Pratap, "Enhancing Bank Security System using Face Recognition, Iris Scanner and Palm Vein Technology," Nov. 2018. doi: 10.1109/IOT-SIU.2018.8519850.

[14] T. Zhu and L. Wang, "Feasibility Study of a New Security Verification Process Based on Face Recognition Technology at Airport," 2019, p. 12025. doi: 10.1088/1742-6596/1510/1/012025.

[15] M. M. Rahman Komol, A. Kumer Podder, A. Arafat, and T. Nabeed, "Remote Sensing Global Ranged Door Lock Security System via Mobile Communication," International Journal of Wireless and Microwave Technologies, vol. 9, no. 5, pp. 25-37, Sep. 2019, doi: 10.5815/IJWMT.2019.05.03.

[16] K. Sadiq et al., "Digitalized Smart Mobile Home Automation and Security System via Bluetooth/Wi-Fi Using Android Platform," International Journal of Information and Communication Sciences, vol. 2, no. 6, pp. 93-99, 2017, doi: 10.11648/j.ijics.20170206.11.

[17] Z. Ahmad, T. S. Ong, T. H. Liew, and M. Norhashim, "Security monitoring and information security assurance behaviour among employees: An empirical analysis," Information and Computer Security, vol. 27, no. 2, pp. 165-188, May 2019, doi: 10.1108/ICS-10-2017-0073/FULL/PDF.

[18] Andreas, C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo, and A. Wibisurya, "Door Security System for Home Monitoring Based on ESP32," Procedia Computer Science, vol. 157, pp. 673-682, Jan. 2019, doi: 10.1016/J.PROCS.2019.08.218.

[19] B. Vaidya, A. Patel, A. Panchal, R. Mehta, K. Mehta, and P. Vaghasiya, "Smart home automation with a unique door monitoring system for old age people using Python, OpenCV, Android and Raspberry pi," in Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems, ICICCS 2017, Jul. 2017, vol. 2018-January, pp. 82-86. doi: 10.1109/ICCONS.2017.8250582.

[20] J. Upadhyay, D. Deb, and A. Rawat, "Design of Smart Door Closer System with Image Classification over WLAN," Wireless Personal Communications, vol. 111, no. 3, pp. 1941-1953, Apr. 2020, doi: 10.1007/S11277-019-06965-Z/FIGURES/9.

[21] A. Ahmed, J. Guo, F. Ali, F. Deeba, and A. Ahmed, "LBPH based improved face recognition at low resolution," 2018 International Conference on Artificial Intelligence and Big Data, ICAIBD 2018, pp. 144-147, Jun. 2018, doi: 10.1109/ICAIBD.2018.8396183.

[22] F. Deeba, A. Ahmed, H. Memon, F. A. Dharejo, and A. Ghaffar, "LBPH-based enhanced real-time face recognition," International Journal of Advanced Computer Science and Applications, vol. 10, no. 5, pp. 274-280, 2019, doi: 10.14569/IJACSA.2019.0100535.

[23] P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," 2004. Accessed: Dec. 02, 2021. [Online]. Available: http://www.merl.com

[24] L. Liu et al., "Deep Learning for Generic Object Detection: A Survey," International Journal of Computer Vision, vol. 128, no. 2, pp. 261-318, Feb. 2020, doi: 10.1007/S11263-019-01247-4/TABLES/2.