Integrating State-of-the-Art Face Recognition and Anti-Spoofing Techniques into Enterprise Information Systems

Satyam Mishra[1], Nguyen Thi Bich Thuy[2], and Cong-Doan Truong[1](✉)

[1] International School, Vietnam National University, Hanoi, Vietnam
satyam.entrprnr@gmail.com, tcdoan@vnu.edu.vn

[2] University of Science, Vietnam National University, Hanoi, Vietnam
nguyenthibichthuy@hus.edu.vn

Abstract. Face Recognition Technology and Face Anti-Spoofing became a necessity during the Covid 19 pandemic, Monkeypox Virus etc. In the current era, the use of contactless technology has become crucial and highly beneficial for individuals. Vietnam is experiencing a significant digital transformation across various sectors including culture, education, tourism, finance, industry, and entertainment. However, most Enterprise Information System institutions in Vietnam lack facial recognition. To address this issue, we have undertaken research to devise a secure anti-spoofing method and determine an effective approach for face recognition processing. Our aim is to develop a comprehensive solution that can be implemented to establish a complete system that we researched and assessed at each stage. To construct a Facial Recognition application, we implemented a Convolutional Neural Network (CNN) as a core to recognize faces in real-time. To identify whether the faces are genuine or counterfeit, we utilized Landmark68 during the anti-spoofing phase. We applied our findings and developed an application AILib during the Covid-19 outbreak, when it was challenging for people to physically visit and login with their IDs at the counter. People can now login without physically being there by logging in using their faces on the AILib. According to the findings of our research, the system functions satisfactorily, with an ideal level of accuracy of 98.42%. Furthermore, we discovered that the optimal threshold value for identifying Asian faces in our face recognition test was determined to be 0.4, while varying threshold values were determined for different face types. For anti-spoofing, during the facial anti-spoofing test, the best threshold value for left, right and front was $d < -50$, $d < -150$ and $d > -50$ respectively, and the right value is $d > -50$ and in comparison, with state-of-the-art methods is pretty good. The program has a high level of practicality, significantly advancing the groundbreaking application of artificial intelligence to enhance people's quality of life and safety.

Keywords: Face Recognition Technology (FRT) · Anti-Spoofing · CNN (Convolutional Neural Network) · Face Landmark/Landmark68

Y. Yang et al. (Eds.): AIMS 2023, LNCS 14202, pp. 71–84, 2023.
https://doi.org/10.1007/978-3-031-45140-9_7

1 Introduction

Face recognition technology (FRT) is a biometric picture capturing tool that's utilized for either identity verification or to recognize an individual to associate them absolutely to their recorded information [1]. For instance, it is frequently employed at the entrances of airport security checkpoints. Although this particular use has its benefits in terms of improved efficiency, its effectiveness relies on the system's processing capability and its specific application [2]. Attendance access control is where face recognition technology finds its widest application in terms of its implementation design [3], security [4] and finance, The areas where face recognition technology is utilized include logistics, retail, smartphones, transportation, education, real estate, government administration, entertainment promotion, and network information security [5–7] and Additional sectors are starting to incorporate face recognition technology. In the realm of security, both the early detection of suspicious incidents and the tracking of suspects can be effectively carried out with the aid of facial recognition [8]. In the field of face recognition technologies and related technologies, there are several stages of development, three of which will be discussed here. The first stage is the Early Algorithm Stage, which includes Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) [9]. Among these algorithms, PCA is widely recognized as the most commonly used method for reducing data dimensionality [10–13]. The second stage, known as the Artificial Features and Classifiers Stage, incorporates various techniques such as Support Vector Machine (SVM), Adaboost, Small Samples, and Neural Networks. On the other hand, the final stage, Deep Learning, is a subset of machine learning that has revolutionized the face recognition industry. Unlike previous stages that require feature extraction, deep learning can automatically identify the necessary features for categorization during the training process. This advancement has had a profound impact on the field of face recognition [14]. Convolutional Neural Network (CNN) falls under one of the categories of face recognition technology. CNN incorporates elements such as localized perception areas, shared weights, and downsampling of facial images to enhance the model structure by leveraging the data's locality and other distinctive characteristics [15]. Some image processing techniques also involve canny edge detection algorithms, quite useful to detect wide range of edges in images [9].

Anti-spoofing refers to the measures taken to counteract spoofing attacks, which involve manipulating data in an attempt to impersonate someone else and gain unauthorized access [16]. The IJCB 2011 competition, which focused on countering 2D facial spoofing attacks, took place recently [17] was a significant group effort for identifying efficient methods for non-intrusive spoofing detection. Multi-modal analysis [18–20], challenge-response technique [21], and multispectral imaging [22] all offer effective ways to distinguish between real and fake faces, However, their practicality is limited due to the requirement for user interaction or specialized imaging requirements. Hence, there is a strong desire to incorporate anti-spoofing techniques into existing face authentication systems that eliminate the need for user cooperation and can utilize standard imaging equipment. One key aspect in verifying the authenticity of a face is the detection of eye blinks, and there are various automated methods available for identifying eye blinks in video frames. Typically, the Viola Jones [23] The operator is employed to detect facial features and landmarks, followed by the utilization of adaptive thresholding to calculate the optical flow surrounding the eyes. Ultimately, by employing a correlation matching template for both open and closed eyes, the eye's motion is estimated.

Since early 2020, the COVID-19 pandemic, triggered by the emergence of the novel SARS-CoV-2 coronavirus, has afflicted the world. Throughout this prolonged period of the pandemic, contactless applications can be implemented by leveraging Face Recognition Technology [24–27]. Amidst the ongoing pandemic, the utilization of Face Recognition technology proves highly beneficial. It eliminates the need for physical presence of students for authentication and allows teachers to mark attendance without having to touch fingerprint scanners. Thang Long University in Vietnam has taken the initiative to test this technology for attendance purposes in classrooms. Their specific face recognition technology, known as "TLnet," automatically identifies and records the faces of students in class [28]. Similarly, Vconnex smart home company launched its face recognition smart lock product which involves face recognition login but lacks security of being spoofed [29]. However, these particular application lacks the capability to prevent face spoofing.

Moreover, in the majority of Enterprise Information System institutions in Vietnam, facial recognition and anti-spoofing technology are not implemented, resulting in employees needing their identity cards to check-in instead of using their faces which is not contact less application; therefore, dangerous during pandemic times. After carefully examining these issues, we have put forth our research proposal to develop a comprehensive system. Our aim was to investigate and evaluate suitable methods for facial recognition processing and secure anti-spoofing measures. We utilized a Convolutional Neural Network (CNN) as the core component for building a real-time Facial Recognition application that detects faces, and incorporated Landmark68 for anti-spoofing to determine the authenticity of a face.

During the Covid-19 pandemic, when physical presence was challenging for people to log in with their IDs at the counter or entrance of Enterprise Information System Institutions, we implemented our research findings and created a user-friendly application called AILib. Now, people can log in to AILib using their faces, eliminating the need to be physically present. The system collects user facial data to enhance the accuracy of face recognition.

Based on our research results, the system has demonstrated satisfactory performance, achieving an optimal accuracy level of 98.42%. Furthermore, we discovered that the best threshold value for Asian faces during face recognition testing was 0.4, while different values applied to other face types. For anti-spoofing, the optimal threshold values for left, right, and front faces were found to be $d < -50$, $d < -150$, and $d > -50$, respectively. This algorithm can be practically applied, making a significant contribution to the innovative application of Artificial Intelligence in improving people's lives, making them safer and more secure.

This paper presents several noteworthy contributions:

a) Creation of a comprehensive system: The authors have developed and implemented a robust system called AILib, which combines facial recognition technology with reliable anti-spoofing measures. This innovative solution allows users to log in using their faces, eliminating the need for physical presence. Particularly during times like Covid-19 and Monkeypox outbreaks, this feature proves advantageous.

b) Utilization of Convolutional Neural Network (CNN) for face recognition: The authors have successfully incorporated CNN as the main component in their real-time face recognition application. This cutting-edge deep learning approach effectively detects crucial facial features without any human intervention.

c) Implementation of Face Landmark/Landmark68 for anti-spoofing: To ensure authenticity and prevent spoofing, the authors have employed the Face Landmark/Landmark68 technique. By analyzing facial landmarks, this system prompts users to perform random actions, making it extremely challenging for fake videos to be used for authentication.

d) Determination of optimal threshold values: Through extensive testing and analysis, the authors have identified ideal threshold values for both face recognition and anti-spoofing across different types of faces. For Asian faces specifically, a threshold value of 0.4 was found to be most effective for face recognition. Additionally, values such as d < -50 for left pose, d < -150 for right pose, and d > -50 for front pose were discovered to enhance anti-spoofing measures.

e) Practical implementation in real-world scenarios: The proposed system has been successfully implemented and rigorously tested in various real-world environments. These practical demonstrations showcase its potential to greatly improve people's lives by offering a secure and convenient authentication method.

2 Methodology

The proposed methodology's architecture as you can see in Fig. 1 comprises several key components. Let's take a closer look:

Front-end Client:

- This is a web-based interface that enables user interaction.
- It captures the user's face using the camera on their device.
- The captured face image is then sent to the back-end server for further processing.

Back-end Server:

- Upon receiving the user's face image from the front-end client, it begins real-time face detection using the Tiny Face Detector Model.
- Facial features are extracted from the detected face utilizing a Deep Convolutional Neural Network (CNN).
- These facial features are encoded into a vector representation, which is then matched with existing face encodings in the database.
- Additionally, it employs the Face Landmark/Landmark68 approach to detect and locate specific facial points such as eyes, nose, and mouth relative to the overall face structure.
- As an added security measure against spoofing attempts, users are prompted to perform random facial expressions like smiling or looking left/right.

Face Database:

- This component serves as a repository for storing and managing facial encodings of registered users.

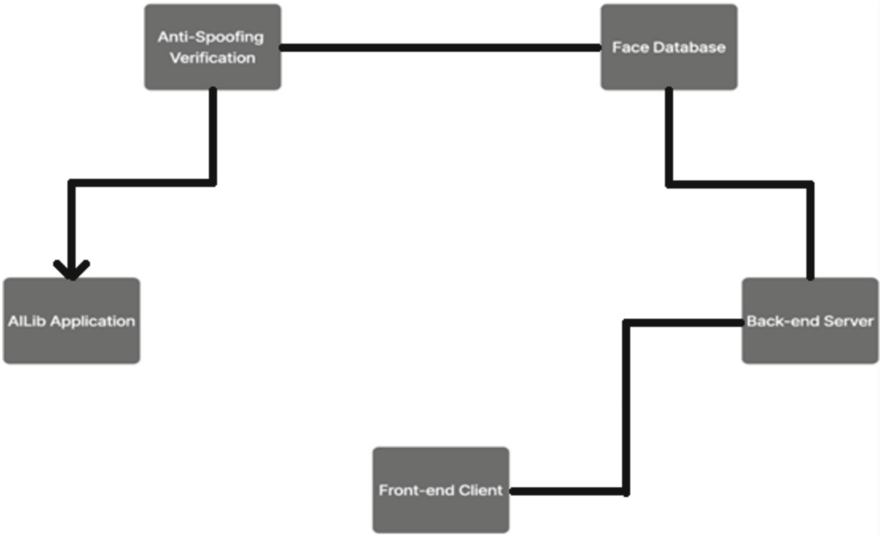


Fig. 1. Proposed Methodology Architecture

- During the face recognition process, these encodings are compared for identification purposes.

Anti-Spoofing Verification:

- To ensure authenticity, this feature measures distances between specific facial points (e.g., point 36 and point 18, point 45 and point 25) in order to detect any noticeable facial movements or changes.
- It analyzes various aspects of facial expressions and movements to verify user authentication.

AILib Application:

- This application provides a user-friendly platform for secure logins.
- Instead of relying on physical presence, users can conveniently log in using their unique facial features.
- Furthermore, regular collection of user facial data helps enhance accuracy over time.

3 Face Recognition Process

3.1 Face Detection

Face detection is a method used to identify the position and dimensions of a person's face within a digital image. It is the initial and crucial step in the process of face recognition. In our research, we utilized the Tiny Face Detector Model to achieve real-time face detection [30]. When it comes to clients with limited resources and mobile devices, our preferred face detector is the Tiny Face Detector. It is highly suitable for mobile platforms and web applications due to its exceptional mobility and compatibility. Additionally, in the realm of automated vehicle research for object detection, the Tiny Yolo V2 model has been employed. This model incorporates depth-wise separable convolutions instead of the conventional convolutions used in Yolo [25, 31].

One of the most widely used and well-known DL networks is the Convolutional Neural Network (CNN) [32, 33]. DL's current popularity can be attributed to CNN, which surpasses its predecessors by autonomously identifying crucial features without the need for human intervention. This ability has made CNN the favored choice and the primary reason behind its widespread adoption. In a variety of fields, such as computer vision [34], audio processing [35], face recognition [36], etc., CNNs have been widely used.

3.2 Face Encoding Process

After receiving the image, the system undergoes the Face Encoding Process, where it analyzes the image, extracts facial features, and represents them in a vector format. This process involves training the system by examining sets of three face images at a time. It generates 128 measurements that capture various facial characteristics such as color, size, slant of eyes, and the distance between eyebrows. To enhance accuracy, slight modifications are made to the neural network, ensuring that the measurements for Image 1 and Image 2 are closer together, while the measurements for Image 2 and Image 3 are further apart. This step is repeated millions of times for millions of images featuring thousands of individuals, allowing the network to consistently generate reliable 128 measurements for each person. Consequently, any set of ten different pictures of the same person should yield the same set of measurements [37].

4 Face Anti-Spoofing Method

4.1 Face Landmark/Landmark68

Facial Landmark refers to the identification of the eye, nose, and mouth's location relative to the overall facial structure. We will search for the primary points that constitute the object's shape within an image. This process consists of two steps: 1. Locating the face within the image, and 2. Detecting the facial structures. Although the face contains numerous key points, our focus will be on essential ones, namely the mouth, right eyebrow, left eyebrow, left eye, right eye, nose, and jaw. The system will utilize the "dlib" library as its foundation [38]. As shown in Fig. 2 below, this method will determine 68 key points that follow the (x, y) coordinates.

As the human face consists of 68 distinct points, any changes in the position of these points will result in a corresponding change in the distance between them. In our system, we leverage this method to prompt users to smile, look left, and look right. We introduce these requirements randomly to prevent users from creating fake videos. To calculate and identify facial movement, we utilize landmark data obtained through an API based on the "dlib" library's landmark. This library can detect the flow of 68 key points with (x, y) coordinates that constitute the human face. Figure 3 illustrates the three poses: frontal, left yaw, and right yaw.

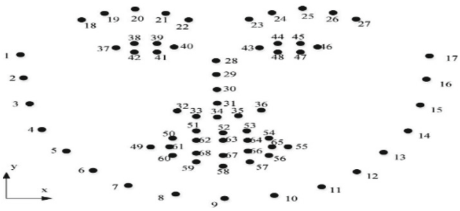


Fig. 2. 68 key points in human face

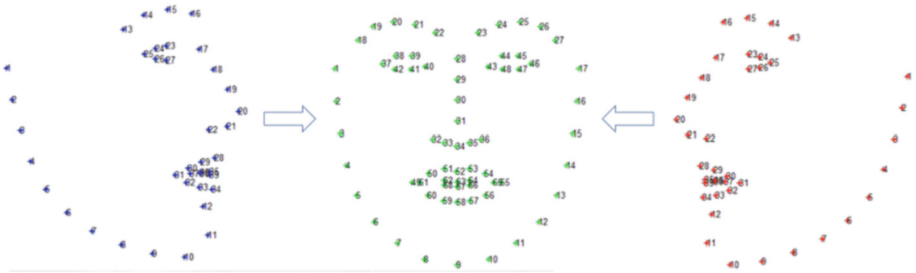


Fig. 3. Face Change Position

Using the face landmark API, we possess the x and y coordinates of 68 essential points on a person's face, each point having a unique value. By measuring the distance between these points, we can detect facial movement accurately. We use Euclidean distance [39] to calculate the distance between each point.

$$d(p, q) = \sqrt{(q1 - p1)^2 + (q2 - p2)^2}$$

Based on Euclidean distance, we can define when the face looks in front of the camera, turn left and turn right to check that the user in front of camera is a real person.

4.2 Face Expression

Two commonly employed approaches for comprehending human emotions involve the analysis of physical or sensory signals. Physical signals include facial expressions, speech, and gestures, while sensory signals contribute to the expression of six fundamental emotions [40]. We can detect the status of human expressions using landmarks and then use this information for various purposes, one of them is anti-spoofing as well. We will use Euclidean distance formula [39] to calculate distance changing from one point to other on facial landmark data to get the facial expression.

5 Proposed Process of Application

In summary, we utilized the Tiny Face Detector Model to detect faces in real-time. Once an image is received, the system begins analyzing it to extract facial features, transforming them into a vector representation. This involved training a Deep Convolutional Neural Network (DCNN) to generate precise measurements of facial features.

The training dataset consisted of three types of images: two images of the same person, two images of different people, and one image of a completely different person. After training, the network became proficient in generating 128 measurements for each person. The person's image stored in the database is then compared with the face image sent by the web client.

Additionally, we employed the Face Landmark/Landmark 68 approach to determine the position of the eyes, nose, and mouth relative to the face. This method involves two steps: first, locating the face in the image, and second, detecting the facial features. By determining the (x, y) coordinates, we establish 68 points on the human face. Any changes in these points will result in changes in the distances between them. To measure these distances, we utilized the Euclidean distance formula [39] in order to determine the authenticity of the user in front of the camera, we employ facial expression analysis to observe any changes.

Within our system, we have incorporated this method as an additional measure by randomly requesting the user to smile, look left, or look right. This approach prevents users from being able to falsify these actions in a video. Within our system, as depicted in Fig. 4, the initial step involves the user accessing the checking client. At this stage, the user will be prompted to gaze into the camera. Subsequently, the client will capture an image and transmit it to the back-end server.

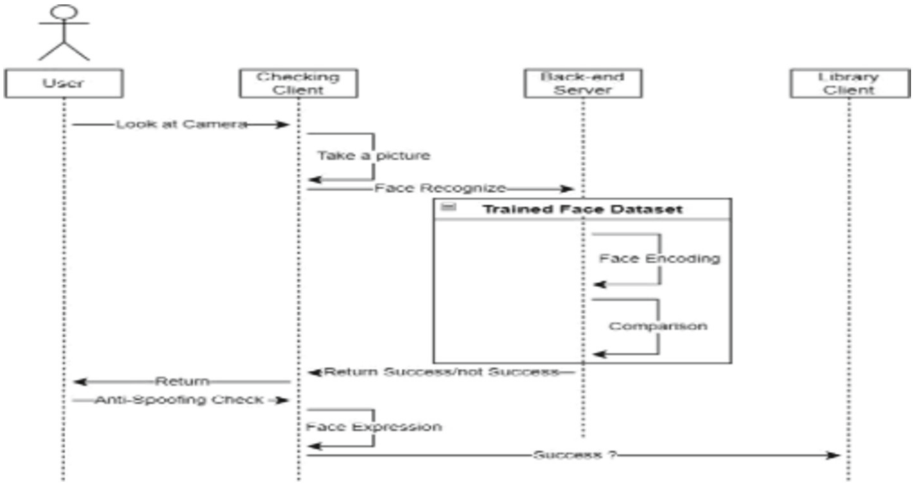


Fig. 4. System Use Case Diagram

This image will be passed to convolutional neural the network model is utilized for training purposes and subsequently, the system encodes the input image to extract facial measurements and compares them with the existing face encodings in the dataset. If the input image matches a pre-existing image, it proceeds to an anti-spoofing process. The user is then prompted to smile or perform a random expression, and once the facial expression is captured, the system verifies the anti-spoofing measures and allows successful login into the user's account on the AILib platform.

6 Results

6.1 Technologies Used

Our system has been specifically designed to incorporate face recognition and anti-spoofing measures. We have implemented face matching in various environments with different lighting conditions. For the front-end and back-end development, we utilized HTML, CSS, and JavaScript to create the web front-end, Python to build the back-end API, Flask as the web framework, and SQLite for storing user information. To enable face-related functionalities such as face detection, landmark68, face expression, and gender recognition, we employed NodeJS along with TensorFlow.js and face-api.js. To ensure accurate face detection and to prevent fake faces, we utilized the Tiny face detector model and landmark68. Additionally, the system underwent two stages of testing: the face recognition test and the face anti-spoofing test.

6.2 The Best Threshold for Application

6.2.1 Face Recognition Threshold Value

To determine the optimal threshold value for face recognition, we conducted two primary steps in a face recognition test: true authentication tests and false acceptance authentication tests. These tests aimed to identify the ideal threshold value and measure the time taken for face recognition. Each individual underwent verification by comparing images captured with various cameras under different lighting conditions. The face recognition time was assessed through 30 trials for each combination of templates and lighting configurations. We tested threshold values of 0.6, 0.55, 0.5, 0.45, and 0.4, repeating each test 100 times to determine the optimal value specifically for Asia Face.

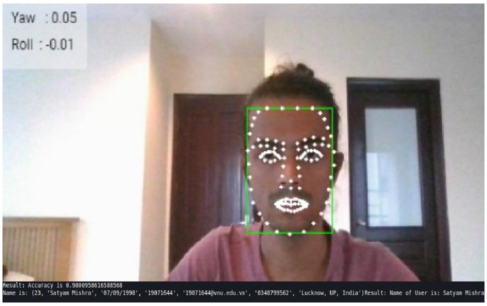
During each trial, the system captured a single frame of face video, loaded the corresponding digital template, searched for a face, and compared it to the existing dataset to find a match. If a match was found, the trial saved the current accuracy before proceeding to the next image in the dataset. The trial concluded once all the subject's face images were scanned, and the highest accuracy achieved was recorded. If no match was found after scanning all the subject's images, the trial stopped and returned a success message stating "not found." In Fig. 4, the system displays the name of the user along with their accuracy and other relevant details when a face match is found.

We performed ten tests using the threshold test case, and for European faces, a tolerance of 0.6 yielded the best results, successfully recognizing individuals with only one to three pictures per subject. However, when applying face recognition to Asia Face, this approach was inaccurate. Table 1 presents the results recorded for face recognition with Asian Face. The system incorrectly recognized the input image when the threshold was set to 0.5 or 0.6. Setting the threshold below 0.5 yielded better results with no incorrect subject identifications. However, in some cases, we were unable to match any subject with a threshold value below 0.45.

We strive to ensure consistency by conducting the tests in the same environment. According to the findings in Table 1, the system with a tolerance of 0.4 is determined to be the most suitable for Asian faces. Figure 5 shows a successful user interface of our research implementation in AILib App.

Table 1. Detect Asian Face with threshold (W- Wrong, R- Right, NF- Not Found)

Threshold	0.6	0.55	0.5	0.45	0.4	0.35	0.3	0.25	0.2	0.1
Result	W	R	W	R	R	R	R	NF	NF	R
	R	W	W	R	R	R	R	NF	R	NF
	W	W	R	R	R	R	NF	R	NF	R
	R	W	R	R	R	R	NF	R	R	NF
	W	R	R	R	R	R	R	R	R	R
	W	R	R	W	R	R	R	R	NF	R
	W	W	W	R	R	NF	R	NF	R	NF
	W	W	W	R	R	R	R	R	R	R
	W	W	R	R	R	R	R	R	R	NF
	W	W	W	R	R	R	R	R	R	R



```
Result: Accuracy is 0.9800958616588568
Name is: (23, 'Satyam Mishra', '07/09/1998', '19071644', '19071644@vnu.edu.vn', '0348799562', 'Lucknow, UP, India')Result: Name of User is: Satyam Mishra
```

Fig. 5. System Encoding Face, performing anti-spoofing and displaying result

6.2.2 Face Anti-Spoofing Threshold Value

During the face anti-spoofing test, three digital templates were employed: the left face, the right face, and the smile face. These trials were conducted to assess the distance between various points on the face. Whenever the face position changed during a trial, the system recorded the values of each facial point within the 68-landmark model, including the distances between point 36 and point 18, point 45 and point 25, and point 63 and point 67.

Based on this, we have conducted calculations to determine the required distance for performing face anti-spoofing. Upon successful spoof checking, the Library Client application appears and displays the recognized user. In our testing, we performed ten trials using the threshold test case, and a tolerance of 0.6 yielded the best results for European faces. For each subject, successful face recognition was achieved with just one to three pictures. However, when it comes to Asian faces, the face recognition results were inaccurate.

Table 2. Value of d

	Left	Front (Smile)	Right
Value of d	−160	−78	−28
	−167	−58	−14
	−164	−56	5
	−178	−98	−39
	−171	−65	−41
	−156	−61	−20
	−167	−91	−44
	−157	−68	−34
	−173	−65	−31
	−155	−103	−15
	−160	−102	−47
	−165	−67	−20
	−153	−74	−45
	−175	−91	−46
	−185	−96	−31
	−188	−97	−43
	−173	−67	−36
	−175	−106	−18
	−178	−90	−42
	−151	−89	−46

In the face anti-spoofing test case, we measured the distance between point 36 and point 18, as well as the distance between point 45 and point 25. We then conducted tests to determine if we could detect the orientation of the face (left or right). As a result of this test case, we obtained three values: "l" represents the value between 36 and 18, "r" represents the value between 45 and 25, and "d" represents the difference between "l" and "r". After conducting ten tests, we recorded values corresponding to a face perpendicular to the camera (smile), a face looking left, and a face looking right. All these values are presented in Table 2.

After conducting 20 tests, we discovered that a front-facing face has a value of "d" less than −50, a left-facing face has a value of "d" less than −150, and a right-facing face has a value of "d" greater than −50. These results are quite favorable when compared to state-of-the-art methods.

7 Conclusion

Our extensive research aimed to develop a comprehensive system involved meticulous evaluation at each stage, focusing on identifying an appropriate facial recognition processing method and implementing a robust anti-spoofing technique. Our efforts were fruitful, resulting in the creation of the AILib application, which was particularly useful during the Covid-19 pandemic. People can now securely login by logging into AILib using their facial features, eliminating the need for physical presence—a particularly advantageous feature during pandemics such as Covid-19 and Monkeypox.

To enhance the accuracy of face recognition, our system collects user facial data. Based on our research findings, the system exhibits satisfactory performance, achieving an optimal accuracy level of 98.42%. Furthermore, we determined that the ideal threshold value for Asian faces during face recognition tests is 0.4, while different thresholds apply to other facial types. Regarding anti-spoofing, our facial anti-spoofing test identified threshold values of $d < -50$ for the left pose, $d < -150$ for the right pose, and $d > -50$ for the front pose.

Further improvements to our system's training and face recognition speed can be achieved by utilizing a client machine and a back-end server. This algorithmic solution holds practical applications and contributes significantly to the pioneering field of Artificial Intelligence, thereby promoting a better and safer way of life. Our research presents a valuable opportunity to modernize existing traditional login/authentication systems by providing users with a convenient and secure means of accessing and protecting their data.

References

1. Lin, S.-H.: An introduction to face recognition technology. Inf. Sci. Int. J. Emerg. Transdiscipl. **3**, 1–7 (2000)
2. Berle, I.: What is face recognition technology? In: Berle, I. (ed.) Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images, pp. 9–25. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-36887-6_2
3. Manjula, V., Baboo, L.: Face detection identification and tracking by PRDIT algorithm using image database for crime investigation. Int. J. Comput. Appl. **38**, 40–46 (2012). https://doi.org/10.5120/4741-6649
4. Lander, K., Bruce, V., Bindemann, M.: Use-inspired basic research on individual differences in face identification: implications for criminal investigation and security. Cogn. Res Princ. Implic. **3**, 26 (2018). https://doi.org/10.1186/s41235-018-0115-6
5. Hu, Y., An, H., Guo, Y., Zhang, C., Zhang, T., Ye, L.: The development status and prospects on the face recognition. In: 2010 4th International Conference on Bioinformatics and Biomedical Engineering, pp. 1–4 (2010). https://doi.org/10.1109/ICBBE.2010.5517197
6. Mishra, S., Vi, P.T., Phuc, V.M., Oni, D., Tanh, N.V.: Using security metrics to determine security program effectiveness. In: Human Factors in Cybersecurity. AHFE Open Acces (2023). https://doi.org/10.54941/ahfe1003720
7. Mishra, S., Phuc, V.M., Tanh, N.V.: Lightweight authentication encryption to improve DTLS, quark combined with overhearing to prevent DoS and MITM on low-resource IoT devices. In: Tekinerdogan, B., Wang, Y., Zhang, L.-J. (eds.) ICIOT 2022. LNCS, vol. 13735, pp. 108–122. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-23582-5_8

8. Mishra, S., Phuc, V.M., Igbagbo, O.D.: BNIS- Bot Node Isolation Strategy to Prevent DoS Attacks: An Improved Overhearing Solution
9. Mishra, S., Thanh, L.T.: SATMeas - object detection and measurement: canny edge detection algorithm. In: Pan, X., Jin, T., Zhang, L.-J. (eds.) AIMS 2022. LNCS, vol. 13729, pp. 91–101. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-23504-7_7
10. Hoyle, D.C., Rattray, M.: PCA learning for sparse high-dimensional data. Europhys. Lett. (EPL) **62**, 117–123 (2003). https://doi.org/10.1209/epl/i2003-00370-1
11. Vijay, K., Selvakumar, K.: Brain FMRI clustering using interaction K-means algorithm with PCA. In: 2015 International Conference on Communications and Signal Processing (ICCSP), pp. 0909–0913 (2015). https://doi.org/10.1109/ICCSP.2015.7322628
12. Vogt, F., Mizaikoff, B., Tacke, M.: Numerical methods for accelerating the PCA of large data sets applied to hyperspectral imaging. Presented at the Proceedings of the SPIE, 22 February (2002). https://doi.org/10.1117/12.456960
13. Ordonez, C., Mohanam, N., Garcia-Alvarado, C.: PCA for large data sets with parallel data summarization. Distrib. Parallel Databases **32**, 377–403 (2013). https://doi.org/10.1007/s10619-013-7134-6
14. Wang, W., Yang, J., Xiao, J., Li, S., Zhou, D.: Face Recognition Based on Deep Learning. In: Zu, Q., Hu, B., Gu, N., Seng, S. (eds.) HCC 2014. LNCS, vol. 8944, pp. 812–820. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-15554-8_73
15. Li, Y., Cha, S.: Implementation of robust face recognition system using live video feed based on CNN. arXiv preprint arXiv:1811.07339 (2018)
16. Schuckers, S.A.: Spoofing and anti-spoofing measures. Inf. Secur. Tech. Rep. **7**, 56–62 (2002)
17. Chakka, M.M. (eds.): Competition on Counter Measures to 2-D Facial Spoofing Attacks (2011). https://doi.org/10.1109/IJCB.2011.6117509
18. Chetty, G., Wagner, M.: Liveness verification in audio-video speaker authentication. In: Proceedings of the 10th ASSTA Conference, pp. 358–363. Macquarie University Press
19. Frischholz, R., Dieckmann, U.: BioID: a multimodal biometric identification system. Computer **33**, 64–68 (2000). https://doi.org/10.1109/2.820041
20. Kollreider, K., Fronthaler, H., Faraj, M.I., Bigun, J.: Real-time face detection and motion analysis with application in “liveness” assessment. IEEE Trans. Inf. Forensics Secur. **2**, 548–558 (2007). https://doi.org/10.1109/TIFS.2007.902037
21. De Marsico, M., Nappi, M., Riccio, D., Dugelay, J.-L.: Moving face spoofing detection via 3D projective invariants. In: 2012 5th IAPR International Conference on Biometrics (ICB), pp. 73–78 (2012). https://doi.org/10.1109/ICB.2012.6199761
22. Pavlidis, I., Symosek, P.: The imaging issue in an automatic face/disguise detection system. In: Proceedings IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications (Cat. No.PR00640), pp. 15–24 (2000). https://doi.org/10.1109/CVBVS.2000.855246
23. Viola, P., Jones, M.J.: Robust real-time face detection. Int. J. Comput. Vision **57**, 137–154 (2004)
24. Coronavirus disease (COVID-19) – World Health Organization. https://www.who.int/emergencies/diseases/novel-coronavirus-2019. Accessed 12 Aug 2022
25. Mishra, S., Minh, C.S., Thi Chuc, H., Long, T.V., Nguyen, T.T.: Automated robot (car) using artificial intelligence. In: 2021 International Seminar on Machine Learning, Optimization, and Data Science (ISMODE), pp. 319–324 (2022). https://doi.org/10.1109/ISMODE53584.2022.9743130
26. Monkeypox cases are rising—here’s what we know so far. https://www.nationalgeographic.com/science/article/monkeypox-cases-are-risingheres-what-we-know-so-far. Accessed 12 Aug 2022
27. Norstrom, P., Consulting, A.: Has Covid increased public faith in facial recognition? Biometric Technol. Today **2021**, 5–8 (2021). https://doi.org/10.1016/S0969-4765(21)00121-1

28. This is the first university in Vietnam to take attendance with face recognition, evasion is only in the past. https://tipsmake.com/this-is-the-first-university-in-vietnam-to-take-attendance-with-face-recognition-evasion-is-only-in-the-past. Accessed 12 Aug 2022
29. News, V.: Báo VietnamNet. https://vietnamnet.vn/en/vietnamese-engineers-develop-face-recognition-smart-lock-2132161.html. Accessed 29 June 2023
30. Hu, P., Ramanan, D.: Finding Tiny Faces (2017). http://arxiv.org/abs/1612.04402
31. Yap, J.W., bin Mohd Yussof, Z., bin Salim, S.I., Lim, K.C.: Fixed point implementation of Tiny-Yolo-v2 using OpenCL on FPGA. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **9** (2018). https://doi.org/10.14569/IJACSA.2018.091062
32. Yao, G., Lei, T., Zhong, J.: A review of Convolutional-Neural-Network-based action recognition. Pattern Recogn. Lett. **118**, 14–22 (2019). https://doi.org/10.1016/j.patrec.2018.05.018
33. Dhillon, A., Verma, G.K.: Convolutional neural network: a review of models, methodologies and applications to object detection. Prog. Artif. Intell. **9**, 85–112 (2020). https://doi.org/10.1007/s13748-019-00203-0
34. Fang, W., Love, P.E.D., Luo, H., Ding, L.: Computer vision for behaviour-based safety in construction: a review and future directions. Adv. Eng. Inform. **43**, 100980 (2020). https://doi.org/10.1016/j.aei.2019.100980
35. Palaz, D., Magimai-Doss, M., Collobert, R.: End-to-end acoustic modeling using convolutional neural networks for HMM-based automatic speech recognition. Speech Commun. **108**, 15–32 (2019). https://doi.org/10.1016/j.specom.2019.01.004
36. Li, H.-C., Deng, Z.-Y., Chiang, H.-H.: Lightweight and resource-constrained learning network for face recognition with performance optimization. Sensors **20**, 6114 (2020). https://doi.org/10.3390/s20216114
37. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning. https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78
38. face-api.js. https://justadudewhohacks.github.io/face-api.js/docs/index.html#models-face-landmark-detection. Accessed 13 Aug 2022
39. Liberti, L., Lavor, C., Maculan, N., Mucherino, A.: Euclidean distance geometry and applications. SIAM Rev. **56**, 3–69 (2014). https://doi.org/10.1137/120875909
40. How to Read Body Language and Facial Expressions. https://www.verywellmind.com/understand-body-language-and-facial-expressions-4147228. Accessed 13 Aug 2022