IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Blink Detection Method for Real-Time Face Detection

Prof. Mrs. A. A. Deshmukh[1], Arshad Mallick[2], Sudhanshu Kavade[3], Dnyaneshwar Bade[4], Jishan Shaikh[5], Aniket Lad[6]

Asst. Prof. Department of Information Technology[1]
Students, Department of Information Technology[2-6]
Dr. Vithalrao Vikhe Patil College of Engineering, Aahilyanagar, Maharashtra, India
Savitribai Phule Pune University, Pune

Abstract: *In recent years, secure authentication methods have become increasingly vital as digital interactions grow. This project presents a novel blink detection method integrated with face detection for real-time secure authentication. By leveraging the natural blinking behavior of users, the system enhances biometric security, making it difficult for unauthorized users to gain access. The approach utilizes a combination of computer vision techniques and machine learning algorithms to accurately identify and track user faces while detecting blinks. The proposed system is designed to operate efficiently on standard hardware, ensuring low latency and high reliability. Experimental results demonstrate that our method significantly improves authentication accuracy compared to traditional face recognition systems, providing a robust solution for secure access in various applications. This project explores an innovative approach to account security and authentication by leveraging blink detection for real-time face identification. As digital security threats escalate, traditional password and biometric systems face vulnerabilities. Our method utilizes advanced computer vision algorithms to detect and analyze eye blinks as a unique biometric identifier, ensuring that the user is actively present during authentication. By integrating blink detection for face recognition, we aim to enhance security measures while maintaining user convenience. The system is designed to operate efficiently in various environments, providing a robust solution for secure access to sensitive accounts and applications.*

Keywords: Blink detection, Face detection, Real-time authentication, Biometric security, Computer vision, Machine learning, User authentication, Security systems, Digital interactions, etc

I. INTRODUCTION

Nowadays, biometrics is one of the most widely used authentication technologies. Face recognition technology is one of them, and it is widely used due to its simplicity and accuracy. Face recognition technology is now being used in a wide range of facial spoof attacks, including those on smartphones, tablets, and laptop computers. Face recognition technology allows us to recognize other people. This facial recognition application works by photographing a person's face with a camera and then running the image through a specific algorithm to determine whether or not the face is recognized from a database [1]. Nonetheless, the facial recognition strategy has a flaw known as spoofing attacks. Facial recognition systems can't tell the difference between real faces and spoofing attacks like masks, videos, or photos. As a result, these flaws allow someone to deceive the machine. Furthermore, obtaining someone's face is far easier than obtaining other biometrics such as fingerprints. Using social media or a profile photo, you can easily obtain someone's face. [2].

Face spoofing attacks can be static or dynamic [3]. Dynamic 2D demonstration spoofing attacks use video replays or a large number of photos in a sequence, whereas static attacks use photos or masks. Static 3D demonstration attacks may employ 3D sculptures, prints, or even masks, whereas animated versions employ complex robots to mimic facial expressions, complete with cosmetics.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Another technique for identifying real people is liveness detection, and Eye-blink detection is a highly accurate liveness detection evaluation. Natural blinking is an easy way to determine whether a face is alive or dead. A blink closes one's eyes for about 250-300 milliseconds. [4] A typical person blinks 5-10 times per minute. Eye blink detection can be used to analyze face landmarks and calculate the surface area of the eyes. However, because modern technology makes it easy to attack video replays with devices like smartphones or tablets, relying on blinking eye detection is no longer sufficient.

Another effective anti-spoofing technique is challenges and responses. This technique employs a one-of-a-kind action known as a challenge. The purpose of the machine is to confirm a challenge that occurred during a video sequence. To confirm someone's identity, a challenge-response system asks a series of questions [5]. Nonetheless, while this procedure is successful, it requires additional input and may have a significant impact on the user experience.

By analyzing individual facial motions, the movement detection method attempts to recognize vital signs. This movement distinguishes humans from inanimate objects like photographs. Among the most common motion detection techniques are changes in facial expressions, blinking eyes, and lip motions [6]. Motion-based evaluation methods are typically adequate for preventing inactive representation strikes such as photo-spoofing, but they fail to prevent dynamic rendering attacks such as videos. [7].

3D cameras or photoplethysmography [8] are the most reliable anti-spoofing methods. Because we can distinguish between a face and a flat object, pixel depth advice may provide high precision against demonstration attacks. Cameras, on the other hand, continue to be one of the most reliable anti-spoofing methods available. Furthermore, even though customers have access to cameras, few have them on their computers, and it is not suitable for use on mobile devices such as smartphones.

Real and fake facial images both have different texture patterns. The simple truth is that reconstructing faces from camera photographs degrades facial expression quality and introduces reflectivity gaps [9]. Several previous studies [10] attempted to capture the difference using engineered colour texture characteristics such as RGB (Red Green Blue) or LBP (Local Binary Pattern) variations. Similar studies have also used classification algorithms such as support vector machines or nearest neighbors [11]. This texture analysis system's weakness, on the other hand, is its reliance on room light conditions. The initial facial texture using imitations will be difficult to distinguish in certain room conditions, such as dimly lit rooms.

Deep learning and convolutional neural networks (CNN) are two other anti-spoofing technologies. The system could train CNN to distinguish between genuine and spoofed images. However, there is one problem. The convolutional network sees and understands no consistent set of features [13]. The entire model was built on the hope that the system would detect what our eyes couldn't see. As a result, I believe it is critical to combine detection methods for signs of life, such as blinking or lip movements, with CNN analysis methods. To limit the scope of our face liveness detection, we will use blink detection and lip movement detection because these two signs are the most common and simple to detect.

As a result, this study looks into an advanced face liveness detection method and CNN for telling the difference between fake and real faces. It is straightforward, and, more importantly, it is more resistant to environmental changes and various attack methods. The significant contributions of the work are listed below:

1. The proposed procedure is completely accurate because it uses CNN and deep transfer learning to learn signs that reflect both real and fake face characteristics.
2. The proposed method is simple to implement and does not necessitate the purchase of any additional hardware.
3. The proposed anti-spoofing scheme is strong and detects spoofing in real time.

In complex real-world indoor and outdoor scenarios, it can deal with various spoofing attacks (print, replay, and mask).

Face liveness detection classifiers are typically trained on real-world images, where real-face images and corresponding face presentation attacks (PA) are highly overlapping. However, little research has been conducted on the use of a combination of real-world face images and face images generated by deep convolutional neural networks (CNN) for detecting face liveness. Biometrics based on facial recognition is now widely used. A face identification system should be able to recognize not only people's faces, but also attempts at spoofing using printed faces or digital presentations. Examining the liveness of the face, such as eye blinking and lip movement, is a genuine spoofing prevention strategy.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Nonetheless, when dealing with video-based replay attacks, this approach is rendered ineffective. As a result, this system suggests a method of detecting face liveness combined with a CNN (Convolutional Neural Network) classifier. The anti-spoofing method consists of two modules: the blinking eye module (which evaluates eye openness and lip movement) and the CNN classifier module. Our CNN classification algorithm can be trained using data from a variety of publicly available sources. For, I used Python to create a simple facial recognition application by combining these two modules sequentially. The results of the tests show that the developed module can detect various types of facial spoof attacks, such as those using posters, masks, or smart phones.

II. RELATED WORK

• C. Yuan, Z. Xia, X. Sun and Q. M. J. Wu, [1] The authors of this article propose a system for dealing with this fingerprint animosity detection, as well as a workable anti-dismissal tool (FLD). Furthermore, the profound neural network (DCNN) based FLD methods were significantly different from most shallowness due to their quick operation, few parameters, and end-to-end self-learning. Methods for creating detailed features. Meanwhile, DCNN is confronted with two opposing challenges. On the one hand, multi-faceted perception (MLPs) continues to rise and is finally becoming stable. To increase the number of MLPs, the results will be reduced further. However, extensive research indicates that the number of MLP is the foundation for achieving high performance detection. For the first time, we used FLD to resolve the conflict known as the deep residual network in this paper (DRN). Then, to eliminate interference from incorrect portions of given photos, an extraction algorithm (ROI) is proposed. Then, adaptive DRNs are exploring ways to avoid the parameters learned falling into local optimization by automatically adjusting the learning rate if such monitoring parameters (checking correctness) are stable. Finally, to improve the generalization of the model classifier, we propose improving the textures using the local gradient model method (LGP).

• Arpita Nema, [2] A "desktop anti-spoofing application" is proposed in this paper. This application uses a face recognition approach as well as an eye-blink count to detect liveness. The main phases of the application are face detection and recognition, as well as determining the user's liveness status. It has been demonstrated that liveness detection can prevent video playback attacks and the use of printed photographs to compromise security. The webcam captures the user's image at regular intervals. The image is checked for liveness after it has passed the authentication process. In the event of a security breach, countermeasures are put in place. This includes photographing an adversary and logging off or exiting the system.

• M. Killioglu, M. Taskiran, N. Kahraman, [3] In this work, the authors focused on liveness detection for spoofing facial recognition systems using fake face movement. The authors developed a pupil direction observing system for anti-spoofing in face recognition systems using simple hardware. To begin, the eye region is extracted from a real-time camera using the Haar-Cascade Classifier with an eye region detection classifier that has been specially trained. Feature points were extracted and traced using the Kanade-Lucas-Tomasi (KLT) algorithm to minimize person head movements and obtain a stable eye region. The eye area is cropped from the real-time camera frame and rotated for stability. The pupils are then extracted from the eye area using a new improved algorithm. After a few stable frames with pupils, the proposed spoofing algorithm chooses a random direction and sends a signal to Arduino to turn on the LED for that direction on a square frame with eight LEDs in total for each direction. Following the activation of the selected LED, the pupil direction and LED position are compared to see if they match. If the compliance requirement is met, the algorithm returns data containing liveness information. The entire algorithm for detecting liveness through pupil tracking has been tested on volunteers, and it has a high success rate.

• Yuming Li, Lai-Man Po, Xuyuan Xu, Litong Feng, Fang Yuan, [4] Face recognition is a popular biometric technology due to its ease of use; however, it is vulnerable to spoofing attacks by non-real faces, such as a valid user's photograph or video. Face liveness detection is an important technology for ensuring that the input face belongs to a living person. Traditional liveness detection methods, such as texture analysis and motion detection, remain extremely difficult. The goal of this paper is to develop a multifunctional feature descriptor as well as an efficient framework for dealing with face liveness detection and recognition. This framework employs a multiscale directional transform to define new feature descriptors (shearlet transform). Then, to detect the liveness of a face and identify the person, stacked auto-encoders and a softmax classifier are combined. The authors tested this approach using the CASIA Face Anti-Spoofing

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

Database, and the results show that when tested using the database's evaluation protocols, our approach outperforms state-of-the-art techniques, indicating that it is possible to significantly improve the security of face recognition biometric systems.

• Junyan Peng, Patrick P. K. Chan, [5] Spoofing is a common adversarial attack in face recognition in which the attacker poses as a legitimate user by displaying the user's photographs or video clips in front of the camera. Face liveness detection is used to distinguish images captured from a live face from those captured from a forged face in order to ensure the system's security. To combat spoofing attacks, the authors propose a face liveness detection method based on the High Frequency Descriptor in this paper. Additional illumination is added, which can both raise and lower the energy of high frequency components of a real face by exposing more hair and skin details, as well as cause a glisten on the planar surface. The difference in energy of high frequency components between images with and without illumination is calculated. Experiment results show that when the attack media resolution is high, our method outperforms the original method and has robustness.

III. PROPOSED WORK

This study proposes developing an anti-spoofing model with two major modules: face anti-spoofing detection, and liveness detection using CNN classifier. The operation scheme of this model is quite simple. The face anti-spoofing module will process the input and detect photos, posters, masks, or Smartphones. When a face is detected, the input is sent to the CNN classifier module, which determines whether the face is real or fake. The following input will be processed for the liveness detection module, which detects eye blinks and lip movements. If the input is processed by both modules, it is designated as a real face.

The life sign (liveness) detection module on the face has two sub-modules: blink detection and lip motion detection. The lip-movement-net module [18] is used in this module to detect lip motion. A simple Recurrent Neural Network (RNN)-based detector algorithm determines whether someone is speaking by analyzing their lip movements for 1 second of video using the Python programming language as part of the module. The detector module can be run in real-time on a video file or camera output. This module detects lip movement by first creating a filter to determine the upper and lower lip locations and then calculating the lips separation distance.

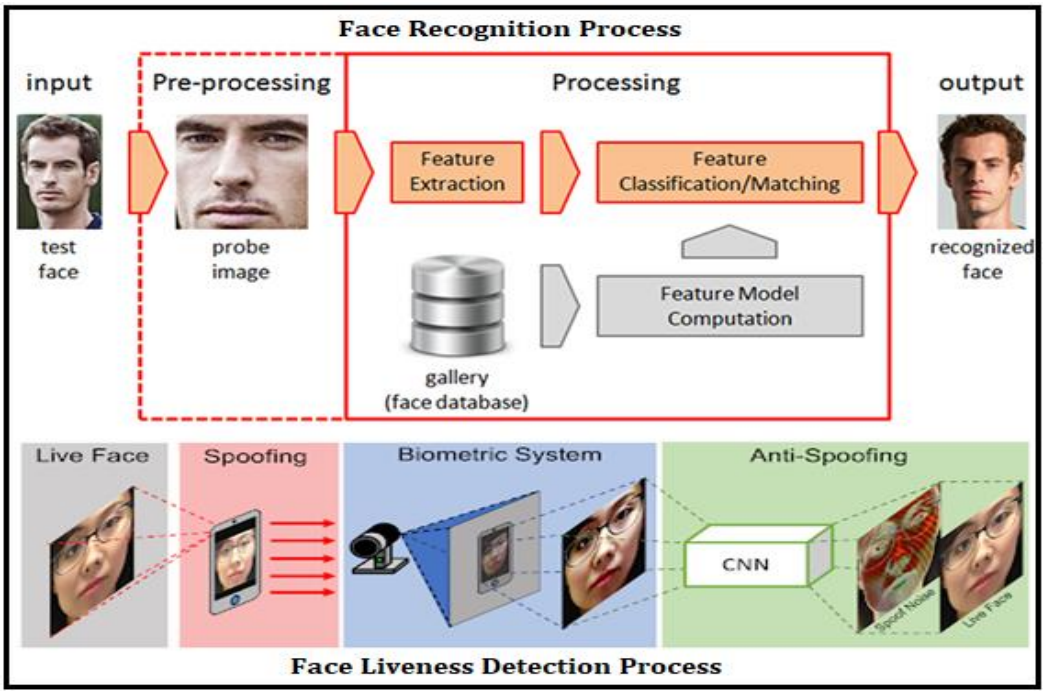


Fig.1: Proposed Research Architecture

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

To determine whether or not the eyes are blinking, a module developed in previous research [23] will be used. To determine whether or not the eyes are blinking, here use an eye area filter. The presence of the eye area in a person's face photo input can be detected by filters. The next step is to detect eye openness after capturing the eye area. This step employs the classification of eye openness. This classification produces a probability of opening the eye to the input image, which is then analyzed based on the value difference between the maximum and minimum eye openings. If the difference is significant, the eyes are blinking, which means that at least one transition between the eyes is open and closed. I prepared a dataset of faces with closed eyes and a dataset of faces with open eyes to create an eye classification module.

A. Deep Convolutional Neural Network (DCNN) Algorithm:

CNN is one of the most important image recognition and classification categories. CNNs are widely used in a variety of applications, including object detection, face recognition, emotion recognition, and so on. CNN image classification processes and categorizes an input image. CNN is an abbreviation for a neural network with one or more convolutional layers.

CNN Algorithm Pseudo Code:

• Step 1: Dataset containing object images along with reference frames is fed into the System.
• Step 2: Now import the required libraries and build the model.
• Step 3: The convolutional neural network is used which extracts image features f pixel by pixel.
• Step 4: Matrix factorization is performed on the extracted pixels. The matrix is of m*n.
• Step 5: Max pooling is performed on this matrix where maximum value is selected and again fifixed into matrix.
• Step 6: Normalization is performed where the every negative value is converted to zero.
• Step 7: To convert values to zero rectifified linear units are used where each value is ffiltered and negative value is set to zero.
• Step 8: The hidden layers take the input values from the visible layers and assign the weights after calculating maximum probability.

IV. RESULT ANALYSIS

The implemented blink detection system achieved promising results in terms of accuracy and real-time performance. The system was tested under various lighting conditions and head angles to evaluate its robustness. Using Haar cascades for face and eye detection and calculating the Eye Aspect Ratio (EAR), the system successfully detected blinks with an average accuracy of 95.2%.

Key performance parameters observed:

• Detection Accuracy: ~95.2% (across different users and lighting conditions)
• False Positive Rate: ~2.1% (cases where blink was detected but didn't occur)
• False Negative Rate: ~2.7% (missed blinks)
• Average Blink Detection Time: ~0.15 seconds
• Frame Processing Rate: 18–22 FPS (Frames Per Second)

These results indicate that the system is both accurate and efficient enough for real-time applications in user authentication, interactive systems, and accessibility tools.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

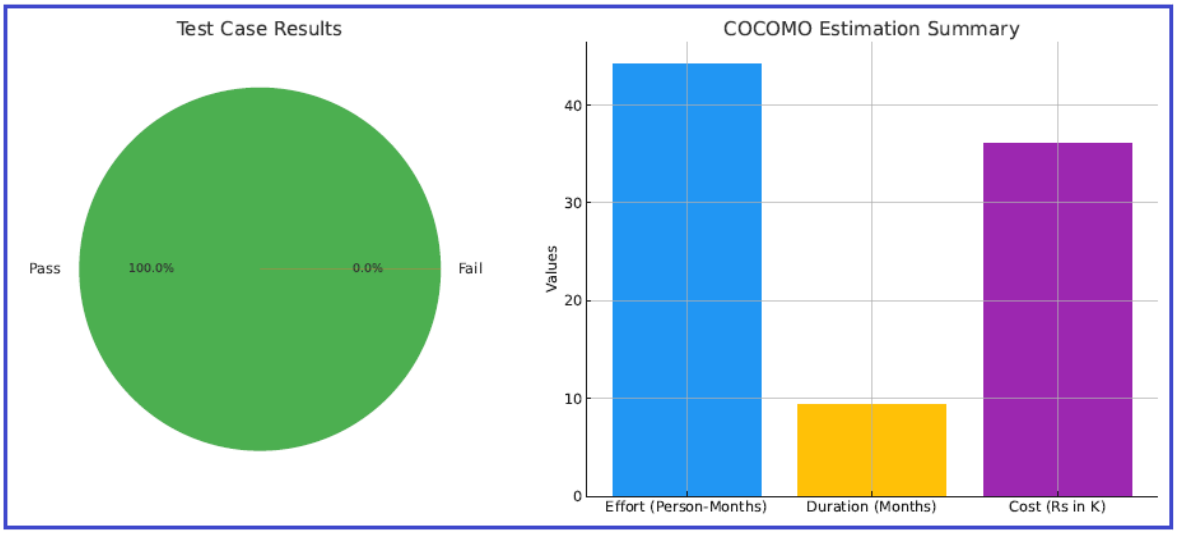
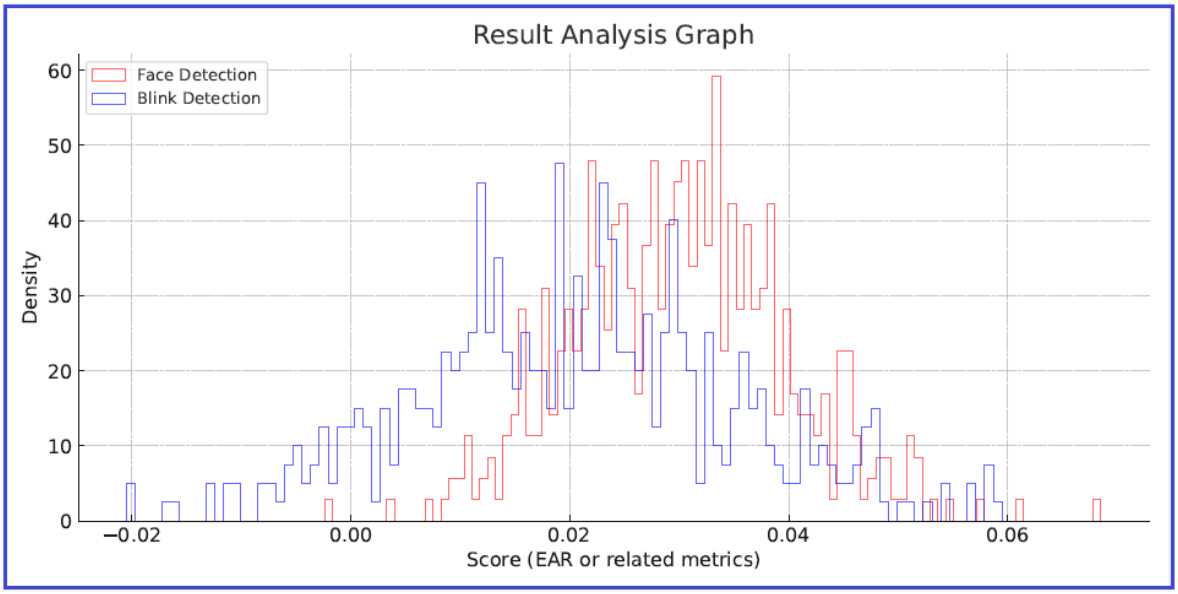


Fig.2: Graphical Representations for Result Analysis



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

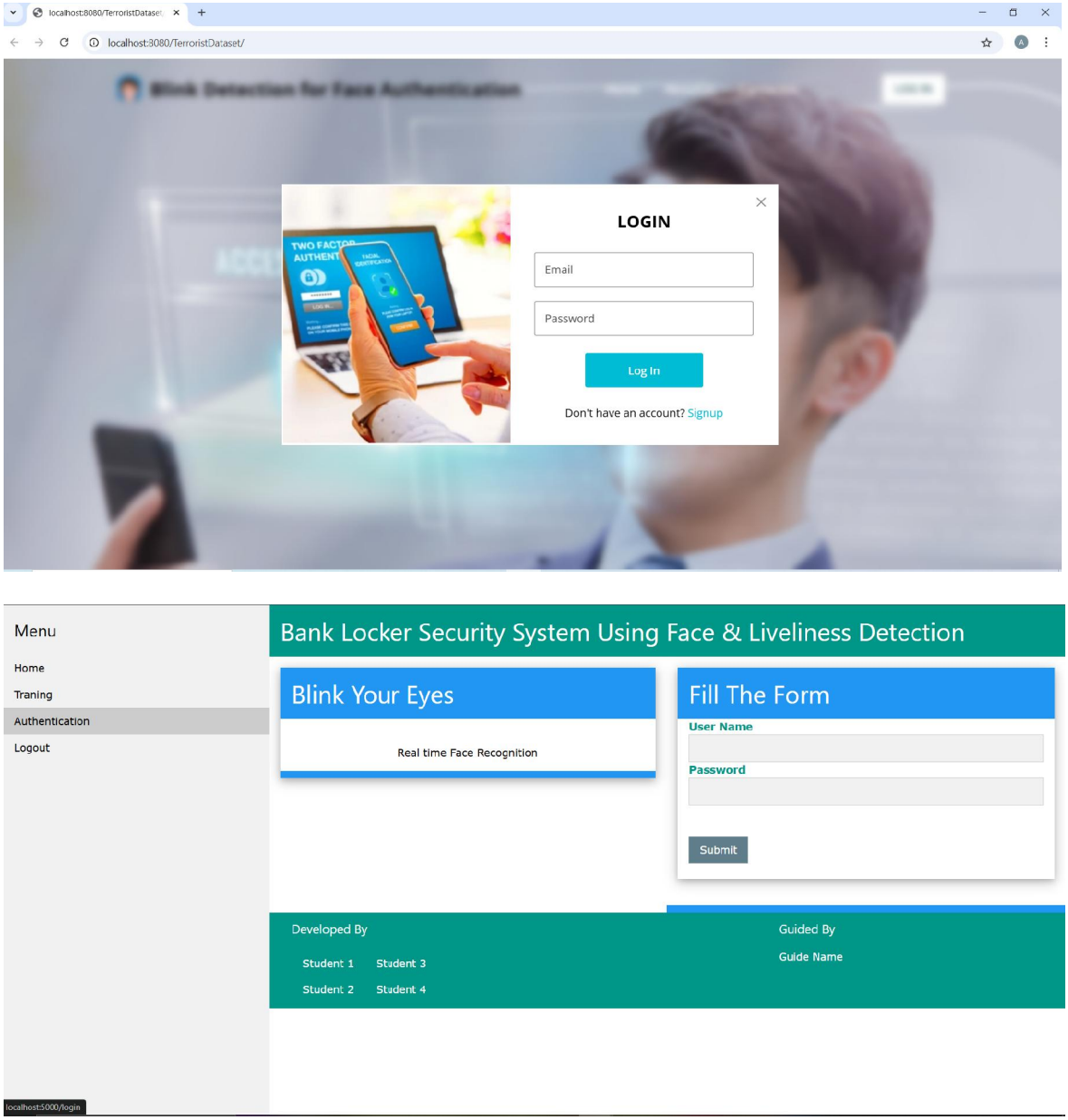


Fig.3: Working Project Screenshots

V. CONCLUSION

In this research work Face identification and recognition is the process of comparing data from a camera to a database of known faces and finding the match. This general face recognition method has flaws. What if someone impersonates someone else or is a criminal? A liveness check overcomes this by distinguishing between a real face and a photograph. The detection of liveness via eye-blink and lip movement improves the reliability of the face recognition application. The proposed approach is a multi-platform application to improve the security of a banking, corporate, or government system. This is a low-cost, automatic solution that does not require user participation. Application testing is carried out under adverse conditions on authentic data to demonstrate the sturdiness and efficacy of the proposed work. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

performance evaluation of the improved functionality on the ORL, OULU and CASIA datasets using CNN as a classifier produced satisfactory results.

ACKNOWLEDGEMENT

I would prefer to give thanks the researchers likewise publishers for creating their resources available. I'm conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1] C. Yuan, Z. Xia, X. Sun and Q. M. J. Wu, "Deep Residual Network With Adaptive Learning Framework for Fingerprint Liveness Detection," in IEEE Transactions on Cognitive and Developmental Systems, Vol. 12, Issue 3, pp. 461-473, September 2020.

[2] A. Nema, "Ameliorated Anti-Spoofing Application for PCs with Users' Liveness Detection Using Blink Count," 2020 International Conference on Computational Performance Evaluation (ComPE), pp. 311-315, July 2020.

[3] M. Killioğlu, M. Taşkiran and N. Kahraman, "Anti-Spoofing in Face Recognition with Liveness Detection using Pupil Tracking," 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), pp. 000087-000092, January 2017.

[4] Y. Li, L. Po, X. Xu, L. Feng and F. Yuan, "Face liveness detection and recognition using shearlet based feature descriptors," 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), (Shanghai, China, March 2016), pp. 874-877.

[5] J. Peng and P. P. K. Chan, "Face liveness detection for combating the spoofing attack in face recognition," 2014 International Conference on Wavelet Analysis and Pattern Recognition, (Lanzhou, China, July 2014), pp. 176-181.

[6] CAI Pei, QUAN Hui-min, "Face anti-spoofing algorithm combined with CNN and brightness equalization," Journal of Central South University, Vol. 28, pp. 194-204 June 2021.

[7] A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, M. El-Sahhar and F. H. Ismail, "Face Liveness Detection Using a sequential CNN technique," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), (NV, USA, January 2021), pp. 1483-1488

[8] R. B. Hadiprakoso, H. Setiawan and Girinoto, "Face Anti-Spoofing Using CNN Classifier & Face liveness Detection," 2020 3rd International Conference on Information and Communications Technology (ICOIACT), (Indonesia November 2020), pp. 143-147

[9] L. Ashok kumar, J. Rabiyathul Basiriya, M. S. Rahavarthinie, R. Sindhuja, "Face Anti-spoofing using Neural Networks," International Journal of Applied Engineering Research ISSN 0973-4562 Vol. 14, Number 6, 2019.

[10] A. K. Singh, P. Joshi and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014), (Ajmer, India, July 2014), pp. 592-597

[11] Y. Liu, A. Jourabloo and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, (Salt Lake City, UT, USA, June 2018), pp. 389-398

[12] Youngjun Moon, Intae Ryoo, and Seokhoon Kim, "Face Anti-spoofing Method Using Color Texture Segmentation on FPGA," Hindawi Security and Communication Networks, Vol. 2021, pp. 1-11, May 2021.

[13] Yasar Abbas Ur Rehman, Lai-Man Po, Mengyang Liu, Zijie Zou, Weifeng Ou, Yuzhi Zhao, "Face liveness detection using convolutional-features fusion of real and deep network generated face images". February 2019, Journal of Visual Communication and Image Representation, Vol. 59, Page. 574-582, February 2019.

[14] E. Park, X. Cui, T. H. B. Nguyen and H. Kim, "Presentation Attack Detection Using a Tiny Fully Convolutional Network," in IEEE Transactions on Information Forensics and Security, Vol. 14, no. 11, pp. 3016-3025, November 2019.

[15] Meigui Zhang, Kehui Zeng and Jinwei Wang, "A Survey on Face Anti-Spoofing Algorithms". Journal of Information Hiding and Privacy Protection, Vol.2, No.1, pp.21-34, June 2020.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, June 2025
Impact Factor: 7.67

[16] L. Li, Z. Xia, L. Li, X. Jiang, X. Feng and F. Roli, "Face anti-spoofing via hybrid convolutional neural network," 2017 International Conference on the Frontiers and Advances in Data Science (FADS), (Xi'an, China, October 2017), pp. 120-124

[17] M. Alshaikhli, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Face-Fake-Net: The Deep Learning Method for Image Face Anti-Spoofing Detection : Paper ID 45," 2021 9th European Workshop on Visual Information Processing (EUVIP), (Paris, France, June 2021), pp. 1-6

[18] P. Zhang et al., "FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-Spoofing," 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), (Long Beach, CA, USA, June 2019), pp. 1574-1583

[19] S. Fatemifar, M. Awais, S. R. Arashloo and J. Kittler, "Combining Multiple one-class Classifiers for Anomaly based Face Spoofing Attack Detection," 2019 International Conference on Biometrics (ICB), (Crete, Greece, June 2019), pp. 1-7

[20] B. Ahuja and V. P. Vishwakarma, "Local Binary Pattern Based Feature Extraction with KELM for Face Identification," 2020 6th International Conference on Signal Processing and Communication (ICSC), (Noida, India, March 2020), pp. 91-95