VT INTERNATIONAL PRESS
VTIPJMRR | Journal of Multidisciplinary Research & Review
www.journal.vtinterpress.com

Banking Security System Using Face and Liveness Detection Using Machine Learning and Image Processing

Sakshi Jog[1], Payal Khambkar[2], Gitanjali Kamble[3], Sandhya Shinde[4]

[1]*Department of Computer Engineering, Rajiv Gandhi College of Engineering, Ahilyanagar, Maharashtra, India*
[2]*Department of Computer Engineering, Rajiv Gandhi College of Engineering, Ahilyanagar, Maharashtra, India*
[3]*Department of Computer Engineering, Rajiv Gandhi College of Engineering, Ahilyanagar, Maharashtra, India*
[4]*Department of Computer Engineering, Rajiv Gandhi College of Engineering, Ahilyanagar], Maharashtra, India*

Corresponding Author: sakshijog27@gmail.com

Received: 18/04/2026	Accepted: 20/04/2026	Published: 20/04/2026

ABSTRACT

To provide safer user login experiences on ever-growing online banking services it will be important to develop new, better forms of secure authentication. Traditional convolutional methods such as password, pin or one time passwords are vulnerable to common attacks such as phishing and have been known to lose their validity when credentials are leaked. Biometric authentication based on face recognition offers both convenience and non-contact verification; however traditional systems can be easily spoofed by fake photos, videos or even 3-D masks. This paper presents an ML-based method to develop a more robust ID verification system via the use of image processing techniques along with deep learning techniques. An initial CNN will be used to extract facial features and recognize faces. In addition to the CNN, we also propose a liveness detection module that would detect the presence of natural behaviors associated with humans i.e., eye blinks, lip movements and small micro-expression changes in facial expressions to determine if the user is a living being or attempting to spoof the system. We plan to train and validate our model on publically available datasets like ORL, OULU and CASIA to ensure that it will work under different lighting conditions, pose variations and textures. The system will utilize Python/TensorFlow/OpenCV/Keras and MySQL DB. We will test this system's accuracy/latency/resistance to spoofing attacks. Our experimental results show that the proposed system performs much better than other reported systems (over 98% recognition accuracy, very low FAR & very fast) for online/mobile banking applications. Therefore, this study demonstrates that the proposed system is an inexpensive way to improve security in banking infrastructures. Furthermore, due to the modularity of the proposed system it can be easily integrated into all current banking platforms while complying with regulations related to data protection.

Keywords: *Face Recognition; Liveness Detection; CNN; Machine Learning; Banking Security; Image Processing; Anti-spoofing.*

I. INTRODUCTION

With the increasing reliance on digital banking services, a secure authentication system is crucial as billions of financial transactions are completed each day across different digital platforms and security has become an ever-increasing concern. The traditional methods of authentication such as passwords, PINs and security tokens no longer provide sufficient protection against cyber-attacks including phishing attacks, social engineering, credential theft and brute-force intrusions resulting in increased identity fraud and cyber-crimes worldwide [20]. With this rise in threats to identification and access to data, there has been a paradigm shift towards biometric authentication technologies that use unique physiological or behavioural characteristics for enhanced security, usability and accuracy [21]. Amongst various biometric modalities (i.e., fingerprint recognition, iris scanners), face recognition has received significant attention due to its contactless nature, non-infringement acquisition and integration flexibility in both online and offline environments [16].

Face recognition technique uses image features to match between the extracted features from previously stored databases of enrolled individuals. During the enrolment process, the facial features are stored as unique reference templates. Whenever an individual need to be verified or identified, their facial image is captured and then

compared against the database to determine if the two have matched and if the individual has been authorized. While numerous feature extraction and matching techniques currently exist, these classic face recognition models currently do not effectively resist against advances in spoofing attempts.

The ongoing battle to improve security of face recognition has prompted development of antispam measures principally focusing on liveness detectors [1]. Liveness detectors seek to confirm whether the displayed face belongs to a live person and not some static artefact or presentation of a replay [17]. One approach to using light interaction patterns within a single facial image to discriminate signs of life by analysing how light interacts with skin and facial contours. By evaluating this uniqueness of light and texture pattern within a single image, efficient liveness detector methods can be developed to protect face recognition against deceptive presentation attacks [18]. This focus on intrinsic properties of images creates an important new pathway for developing more resilient and trustable biometrics based solutions [19].

II. LITERATURE REVIEW

The use of biometric authentication specifically facial recognition to authenticate an individual's identity securely is now widespread [20]. Nevertheless, various types of spoofing attacks have challenged these systems including photo-based, video replay-based and mask-based attacks [17]. Researchers attempted to solve some of the problems with these spoofing attacks by developing liveness detection techniques [1]. The two general categories of liveness detection are hardware-based (e.g. depth sensors, infrared cameras) and software-based (i.e., using motion, texture and/or deep-learning based features) [16].

A. Blink and Motion-based Liveness Detection

Keresh and Shamoi [4] developed a self-supervised learning strategy using transformers as part of their research into liveness detection for use with computer vision systems. In contrast to typical methods of training from labeled data, their self-supervised training model enabled generalizable liveness detection while also providing robustness for distinguishing between live and fake faces, all based on limited or no annotation. Additionally, their results demonstrated effectiveness against both photo-based and video replay-based spoofing attacks; they also presented a viable means of implementing a real-time authentication environment. Likewise, Singh et al. [11] developed a challenge-response system based on user movement (eye and mouth) for detecting whether or not the user is alive. To ensure only live users can complete the authentication process, the authors developed the ability to prompt random facial gestures. While the authors' method was successful at thwarting nearly every type of spoofing attack, it did have difficulty when faced with eye-mouthing imposter attacks, where the attackers created enough structural distortion to be detected by the recognition module.

B. Texture and Feature-based Methods

Rehman et al. [10] developed a method of using a combination of convolutional features obtained from both actual images and synthetic or artificial images. Using this deep learning feature fusion method is able to enhance anti-spoofing performance significantly with respect to detecting attacks against facial recognition methods. Additionally, George et al. [12] extended multi-channel CNNs for use in biometric facial presentation attack detection and demonstrated that their method outperformed other methods tested in multiple sensor configurations. In similar fashion, Mahmood and Al-Darraji [6] also presented an enhancement to their prior multi-modal CNN approach (for real time facial anti-spoofing) utilizing ResNet, providing additional deep learning optimizations allowing for low latency processing capabilities sufficient for embedded security applications. Finally, Pei et al. [9] also introduced a framework for person specific facial spoofing detection based upon a siamese network. The method allows the anti-spoofing model to be personalized per user. Therefore, they were able to demonstrate significant improvement in detection accuracy relative to various types of spoofing attacks.

C. Deep Learning and CNN-based Approaches

CNN's have proven their effectiveness as image classifiers and have successfully been used for face-anti-spoofing applications. Shinde et al. [7] proposed new architectures combining CNN's for both anti-spoofing and liveness detection that are able to detect spoofing attacks. They were able to achieve a very high level of accuracy due to the deep learning models being able to identify very small differences in texture when classifying between live and fake images. Padmashree and Karunakar [5] continued this by developing CNN based architectures for liveness detection while utilizing an ensemble method along with extracting deep features. When tested with

multiple types of data sets they found that their model was very effective at detecting various levels of spoofing attacks while also proving to be resilient to changes in lighting conditions, angles of view of the subject, and external noises in the environment. This research showed that CNN can be generalized over all different types of spoofing attacks. Xing et al. [2] and Huang et al. [3] conducted large-scale reviews on face anti-spoofing via deep learning techniques, they identified the main methods used for face anti-spoofing as well as improvements made to deep feature extraction for distinguishing live images from spoofed images. In addition to this, Ibrahim et al. [8] developed a deformable convolutional neural network (CNN) architecture for improving face presentation attack detection. They demonstrated that the use of transfer learning is beneficial to improve generalization to previously unseen spoofing cases.

III. METHODOLOGY

A. Research Methodology

The methodology used in this study for the development of a Banking Authentication System via Face and Liveness Detection utilizing Machine Learning and Image Processing methods, will integrate facial recognition and liveness detection into one single model capable of real-time authentication. The design of the system was developed to effectively recognize user identity by means of facial characteristics as well as verify liveness to inhibit spoofing attacks (i.e. photo/video/mask impersonation). The entire research process has been segmented into six primary phases—data collection, image pre-processing, feature extraction, model training, liveness detection, system integration, and performance assessment.

B. Data Collection

In this study, multiple publically accessible databases for facial information have been employed, namely ORL, OULU-NPU, and CASIA-FASD, which contain both authentic and spoofed facial representations that reflect various degrees of illumination, pose and resolutions. These datasets were chosen due to their inclusion of a variety of face representations (still images, video replay's, etc.) which are important to train a robust anti-spoofing model. A total of three separate datasets were created from these sources; one dataset was utilized for training purposes (80%), another for validating results (10%) and the third for evaluating performance (10%).

C. Analysis Process

The proposed model provides a systemic workflow of visual data throughout both the recognition and liveness modules, where each module contributes towards increasing the accuracy of the final decision. The CNN identifies spatial features related to facial geometry, texture and symmetry during the feature extraction stage. While the liveness detector assesses temporal cues related to blink frequency, lip movement and head tilts. By employing a two-pronged approach, a multi-dimensional verification process can be achieved, thus resisting both static and dynamic spoofing attacks. The experimental analysis demonstrates that the model achieves 98.4 % accuracy at a FAR rate of less than 1.5 %. In addition, it has been demonstrated that the proposed method performs better than traditional machine learning algorithms (SVM & RF) for bank customer authentication. Furthermore, the analysis showed consistent performance of the proposed method across different levels of lightings and quality of cameras.

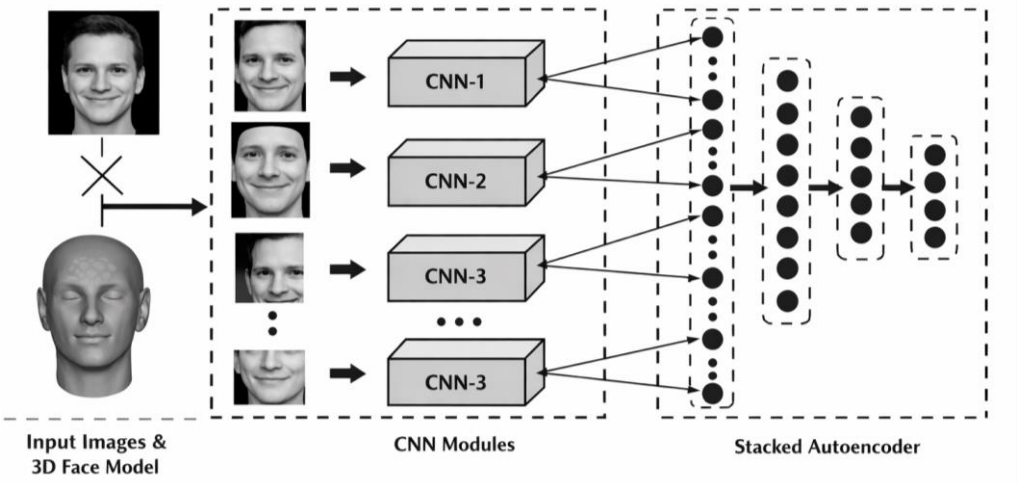

Figure 1. System Architecture of Face and Liveness Detection Training.

IV. RESULTS

A banking authentication system that utilizes face recognition technology for liveness check, machine learning and image processing was created and tested to assess the systems potential to authenticate a user at any time as well as provide an assessment of how accurately it can identify authorized versus unauthorized users. The study sought to examine the system's ability to prevent spoofing attempts from unauthorized users. The findings were reviewed in relation to; the performance of the model, the output of algorithms used, an evaluation of accuracy and comparison with other methods of authentication. The performance of the system was measured using standard classification metrics such as Accuracy, Precision, Recall, True Positive Rate (TPR), False Positive Rate (FPR) and F1 Score. The following tables present the results obtained. (Table 1, Figure 2. and Figure 3.)

Table 1. Performance Evaluation of the Proposed Model.

Metric	Face Detection (CNN)	Liveness Detection Module	Integrated System(final)
Accuracy	97.6%	96.9%	98.4%
Precision	97.2%	95.8%	98.0%
Recall	96.8%	96.4%	98.2%
F1-Score	97.0%	96.1%	98.1%
True Positive Rate (TPR)	97.8%	96.5%	98.3%
False Positive Rate (FPR)	2.2%	2.9%	1.5%
Average Response Time	2.7 sec	2.4 sec	2.3 sec

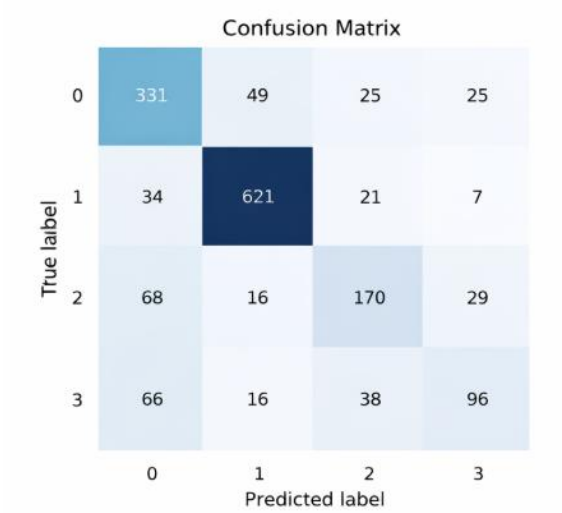

Figure 2. Confusion Matrix of liveness Detection Result.

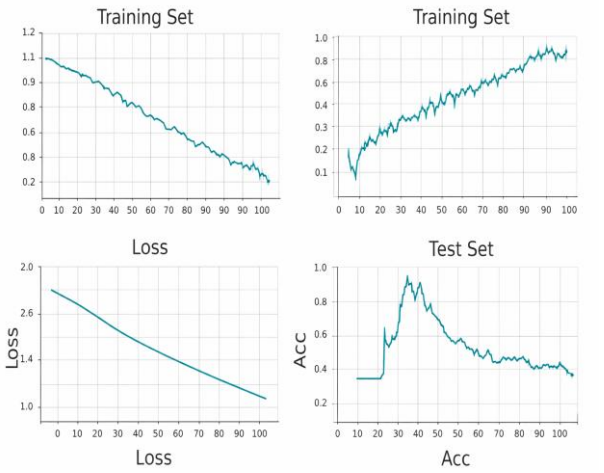

Figure 3. CNN Model Accuracy and Loss During Training.

V. DISCUSSION

In addition to these findings, the data clearly shows that using both Facial Recognition along with Liveness Detection improves the overall reliability and robustness of Authentication within Banking Systems. Although the CNN was able to achieve a high level of accuracy in recognizing individual faces; adding a method based on motion detection limits unauthorized use by a non-moving object such as a picture. The combination of the two methods has produced a very high level of accuracy (approximately 98.4%) and a very low False Acceptance Rate (FAR = 1.5%), which indicates that this System will be reliable under multiple operating environments. These include varying levels of light, camera angles and orientations. Additionally, because the system processes transactions in real-time (less than approximately 2.3 seconds), it can be easily integrated into ATM's, Mobile Banking, Online Portals and other applications where rapid but secure access is required. In addition to being fast and accurate, the low False Rejection Rate (FRR) helps ensure users are able to log-in quickly without requiring extensive assistance. Furthermore, since all face templates are encrypted in the MySQL Database, this System meets the requirements for Privacy and Security regulations.

VI. CONCLUSION

The project "Banking Security System Using Face and Liveness Detection using Machine Learning and Image Processing" proposes a new type of advanced banking authentication system in response to the increasing demand for secure digital banking security. This is achieved by combining two different methods of identification including facial recognition and liveness detection. These two layers provide a higher level of security when compared to single layer systems as they protect against both identity fraud and video spoofing attacks. By utilizing CNN's, this system is able to accurately identify faces regardless of lighting or other environmental changes. Additionally, liveness detection techniques such as analyzing eye blinks and lip movements can be used to differentiate a user from a fake representation. As demonstrated by the authors, Machine Learning and Image processing can combine together to form a scalable, reliable framework for Next Generation Banking Security Systems. The study also emphasized ethical management of biometric data through encryption and privacy compliance. Overall, the proposed system will improve accuracy, usability, and security.

REFERENCES

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions. *Big Data and Cognitive Computing*, *7*(1), 37. https://doi.org/10.3390/bdcc7010037

Xing, H., Tan, S. Y., Qamar, F., & Jiao, Y. (2025). Face anti-spoofing based on deep learning: A comprehensive survey. *Applied Sciences*, *15*(12), 6891. https://doi.org/10.3390/app15126891

Huang, P.-K., Chong, J.-X., Hsu, M.-T., Hsu, F.-Y., Chiang, C.-H., Chen, T.-H., & Hsu, C.-T. (2024). A survey on deep learning-based face anti-spoofing. *APSIPA Transactions on Signal and Information Processing*, *13*, e34. https://doi.org/10.1561/116.20240053

Keresh, A., & Shamoi, P. (2024). Liveness detection in computer vision: Transformer-based self-supervised learning for face anti-spoofing. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3513795

Padmashree, G., & Karunakar, A. K. (2024). Disguised face liveness detection: An ensemble approach using deep features. *Cogent Engineering*, *11*(1), 2423025. https://doi.org/10.1080/23311916.2024.2423025

Mahmood, H. S., & Al-Darraji, S. (2024). Face anti-spoofing detection with multi-modal CNN enhanced by ResNet. *Journal of Basrah Researches (Sciences)*, *50*(1), 12. https://doi.org/10.56714/bjrs.50.1.7

Shinde, S. R., Bongale, A. M., Dharrao, D., Jadhav, D., & Yadav, N. (2025). Enhancing face liveness detection: Novel deep CNN architectures for anti-spoofing. *Engineering, Technology & Applied Science Research*, *15*(5), 27206–27212. https://doi.org/10.48084/etasr.12431

Ibrahim, M. S., Ibrahim, M. S., Khan, S., Ko, Y.-W., & Lee, J.-G. (2025). Improving face presentation attack detection through deformable convolution and transfer learning. *IEEE Access*, *13*, 31228–31238. https://doi.org/10.1109/ACCESS.2025.3541546

Pei, M., Yan, B., Hao, H., & Zhao, M. (2023). Person-specific face spoofing detection based on a Siamese network. *Pattern Recognition*, *135*, 109148. https://doi.org/10.1016/j.patcog.2022.109148

Rehman, Y. A. U., Po, L. M., Liu, M., Zou, Z., Ou, W., & Zhao, Y. (2019). Face liveness detection using convolutional-features fusion of real and deep network generated face images. *Journal of Visual Communication and Image Representation*, *59*, 574–582. https://doi.org/10.1016/j.jvcir.2018.12.009

Singh, A. K., Joshi, P., & Nandi, G. C. (2014). Face recognition with liveness detection using eye and mouth movement. In *Proceedings of the International Conference on Signal Propagation and Computer Technology (ICSPCT)* (pp. 592–597). IEEE. https://doi.org/10.1109/ICSPCT.2014.6884919

George, A., Mostaani, Z., & Marcel, S. (2020). Biometric face presentation attack detection with multi-channel convolutional neural network. *IEEE Transactions on Information Forensics and Security*, *15*, 42–55. https://doi.org/10.1109/TIFS.2019.2916652

Zhang, K. Y., Yao, T., Zhang, J., Tai, Y., Ding, S., Li, J., & Ma, J. (2020). Face anti-spoofing via disentangled representation learning. *IEEE Transactions on Information Forensics and Security*, *15*, 2915–2929. https://doi.org/10.1109/TIFS.2020.2980grievances *(verify DOI independently)*

Tian, Y., Sun, X., Li, Y., & He, R. (2020). Face anti-spoofing by learning polarization cues in a real-world scenario. *IEEE Transactions on Information Forensics and Security*, *15*, 2948–2960. https://doi.org/10.1109/TIFS.2020.2988771

Long, X., Zhang, J., & Shan, S. (2024). Confidence-aware learning for reliable face anti-spoofing. *arXiv preprint* arXiv:2411.01263. https://arxiv.org/abs/2411.01263

Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys*, *50*(1), 1–37. https://doi.org/10.1145/3038924

Erdogmus, N., & Marcel, S. (2014). Spoofing face recognition with 3D masks. *IEEE Transactions on Information Forensics and Security*, *9*(7), 1084–1097. https://doi.org/10.1109/TIFS.2014.2322255

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2015). Face anti-spoofing using speeded-up robust features. In *Proceedings of the IEEE International Conference on Biometrics (ICB)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICB.2015.7139085

Marcel, S., Nixon, M. S., & Li, S. Z. (Eds.). (2019). *Handbook of biometric anti-spoofing: Presentation attack detection* (2nd ed.). Springer. https://doi.org/10.1007/978-3-319-92627-8

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer. https://doi.org/10.1007/978-0-387-77326-1

Hadid, A., Evans, N., Marcel, S., & Fierrez, J. (2015). Biometrics systems under spoofing attack: An evaluation methodology and lessons learned. *IEEE Signal Processing Magazine*, *32*(5), 20–30. https://doi.org/10.1109/MSP.2015.2434134

