INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1396-1403

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

BANKING AUTHENTICATION SYSTEM POWERED BY FACE RECOGNITION AND LIVENESS CHECK VIA ML AND IMAGE PROCESSING

Jog Sakshi Vinayak[1], Khamkar Payal Rahul[2], Kamble Gitanjali Subhash[3], Shinde Sandhya Laxman[4], Prof. Unde Suvarna Popat[5]

[1,2,3,4]Student (B.E.), Department Of Computer Engineering, Rajiv Gandhi College Of Engineering, Karjule Harya, Maharashtra, India.

[5]Asst. Prof., Department Of Computer Engineering, Rajiv Gandhi College Of Engineering, Karjule Harya, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS44440

ABSTRACT

The primary purpose of this research is to develop a secure and intelligent banking authentication system that integrates face recognition with liveness detection to prevent identity fraud and unauthorized access in digital financial services. Traditional authentication methods such as passwords, PINs, and tokens are prone to phishing and cyberattacks, while conventional facial recognition systems can be easily deceived by printed photos, replayed videos, or 3D mask attacks. To address these limitations, this study proposes a Machine Learning–based approach utilizing Image Processing and Deep Learning techniques for robust identity verification. The system is designed using a Convolutional Neural Network (CNN) for accurate facial feature extraction and recognition, combined with a liveness detection module that analyzes natural human behaviors such as eye blinking, lip movement, and subtle facial micro-expressions to differentiate between live users and spoofing attempts. The model is trained and validated using publicly available datasets such as ORL, OULU, and CASIA, ensuring adaptability to diverse illumination, pose, and texture conditions. The implementation, developed in Python using TensorFlow, OpenCV, and Keras with a MySQL database, was tested for accuracy, latency, and resilience to spoofing attacks. Experimental analysis demonstrated that the proposed system achieved superior performance with over 98% recognition accuracy, a low false acceptance rate (FAR), and real-time response suitable for online and mobile banking environments. The results indicate that combining CNN-based recognition with motion-aware liveness verification significantly enhances authentication reliability compared to traditional methods. The study concludes that the proposed system provides a cost-effective, efficient, and user-friendly solution that strengthens banking security infrastructure. Moreover, its modular design allows seamless integration with existing banking platforms while ensuring data privacy and regulatory compliance. Overall, the research establishes that fusing machine learning and image processing techniques can revolutionize biometric security, setting a foundation for next-generation banking systems capable of resisting evolving digital spoofing and fraud attempts.

Keywords: Face Recognition, Liveness Detection, Machine Learning, Image Processing, Convolutional Neural Network (CNN), Banking Security, Biometric Authentication, Spoofing Detection, Deep Learning, Cybersecurity, Artificial Intelligence (AI), Eye Blink Detection, Lip Movement Analysis, Real-Time Authentication, Fraud Prevention.

1. INTRODUCTION

In today's digital era, the banking and financial sectors are increasingly dependent on technology-driven services that require secure, reliable, and efficient user authentication systems. With the growth of internet and mobile banking, billions of financial transactions occur daily across digital platforms, making security a critical concern. Traditional authentication methods such as passwords, PINs, and security tokens are no longer sufficient to safeguard sensitive data and prevent unauthorized access. These conventional systems are vulnerable to phishing attacks, social engineering, credential theft, and brute-force intrusions, leading to a surge in identity fraud and financial crimes worldwide. As a result, there has been a paradigm shift toward **biometric authentication** technologies that rely on unique physiological or behavioral traits, offering enhanced security, usability, and accuracy. Among various biometric modalities, **face recognition** has gained significant attention due to its contactless nature, non-intrusive acquisition, and integration flexibility in both physical and online environments.

However, despite its advantages, face recognition systems face a major challenge—**spoofing attacks**—where attackers use printed photographs, digital screens, or three-dimensional masks to impersonate genuine users. Such

vulnerabilities severely undermine the reliability of face-based authentication, particularly in critical sectors such as banking, finance, and e-commerce. Consequently, researchers have focused on developing **face liveness detection** techniques that can distinguish between live faces and spoofed media by analyzing subtle movements and texture variations. Liveness detection ensures that the system recognizes not just a face, but a *living* face exhibiting natural behaviors such as eye blinking, lip motion, and spontaneous micro-expressions. Integrating liveness detection with face recognition thus provides a dual-layer security mechanism capable of resisting presentation attacks and enhancing trust in automated verification systems.

Recent advancements in **Machine Learning (ML)** and **Deep Learning (DL)** have revolutionized the way computers interpret visual data, enabling robust and intelligent systems for real-time facial analysis. In particular, **Convolutional Neural Networks (CNNs)** have demonstrated remarkable performance in image classification, object detection, and facial feature extraction. CNN-based models can automatically learn complex hierarchical patterns and subtle differences between real and spoofed faces without the need for manual feature engineering. Furthermore, the incorporation of **image processing techniques** such as normalization, edge detection, and texture mapping enhances the accuracy and speed of recognition, even under challenging environmental conditions like varying illumination or occlusion. The convergence of these technologies has opened new research directions in developing secure, AI-driven facial authentication systems.

Current studies in this domain focus on developing efficient algorithms for **anti-spoofing** and **liveness detection** using deep neural architectures. Research by various scholars has introduced hybrid models that combine spatial and temporal information to detect facial motion, surface texture, and reflectance differences between real and artificial faces. Databases such as CASIA-FASD, OULU-NPU, and Replay-Attack have become benchmarks for testing face liveness detection algorithms, allowing researchers to measure performance against diverse attack scenarios. Despite these advancements, there remains a pressing need for systems tailored to real-world applications—particularly in **banking environments**, where authentication must balance accuracy, speed, and user convenience. Banking systems demand real-time responses, minimal latency, and strict compliance with data security standards, making the design of a scalable and trustworthy face recognition model both a technical and ethical necessity.

This study explores the integration of **Face Recognition** and **Liveness Detection** within the banking domain using Machine Learning and Image Processing techniques. The proposed system employs a CNN-based architecture to identify and authenticate users based on their facial characteristics while simultaneously verifying liveness through dynamic motion and texture cues. By combining facial recognition and behavioral verification, the research aims to minimize spoofing vulnerabilities and enhance the reliability of digital banking transactions. Ultimately, this work contributes to the growing field of AI-based biometric security, proposing a model that ensures **real-time, accurate, and fraud-resistant authentication**—a vital requirement for next-generation financial technologies and digital trust infrastructure.

2. METHODOLOGY

The methodology adopted in this research focuses on developing a **Banking Authentication System using Face and Liveness Detection** through **Machine Learning** and **Image Processing** techniques. The proposed approach integrates facial recognition and liveness detection into a unified model capable of real-time authentication. The system is designed to accurately identify users based on facial features while simultaneously verifying liveness to prevent spoofing attacks such as photo, video, or mask impersonations. The overall research process is divided into several key phases—data collection, image preprocessing, feature extraction, model training, liveness detection, system integration, and performance evaluation.

2.1 Data Collection:

The research utilizes multiple publicly available face datasets, including **ORL**, **OULU-NPU**, and **CASIA-FASD**, which provide both genuine and spoofed facial samples under varying illumination, pose, and resolution conditions. These datasets were selected because they include diverse face presentations such as still images, video replays, and printed photographs, which are essential for training a robust anti-spoofing model. The datasets are divided into training, validation, and testing sets in an 80:10:10 ratio to ensure balanced learning and unbiased evaluation.

2.2 Image Preprocessing:

Preprocessing plays a vital role in improving the quality and consistency of input images before feeding them into the model. Each image undergoes several enhancement operations, including **image resizing**, **histogram equalization**, **Gaussian blurring**, and **normalization** to standardize pixel intensity. **Face detection** is performed using Haar Cascade and Dlib libraries to isolate the region of interest (ROI). This step eliminates background noise and ensures

that only relevant facial features are analyzed. The preprocessed images are then converted into grayscale to reduce computational complexity without compromising the integrity of feature extraction.

2.3 Feature Extraction using CNN:

Feature extraction is implemented through a **Convolutional Neural Network (CNN)** that automatically learns hierarchical representations of facial features. The CNN architecture consists of multiple convolutional layers followed by ReLU activation, pooling layers for dimensionality reduction, and fully connected layers for classification. The convolutional layers extract low-level features such as edges and textures, while deeper layers learn high-level features like eye shape, nose structure, and facial contours. The **Softmax classifier** is applied in the final layer to classify faces as either *authorized* or *unauthorized*. The CNN model is trained using **cross-entropy loss** and optimized with the **Adam optimizer** to ensure fast convergence and prevent overfitting.

2.4 Liveness Detection Module:

To counter spoofing attacks, a **liveness detection module** is integrated into the system. This module analyzes dynamic facial movements such as **eye blinking**, **lip motion**, and **facial micro-expressions** to determine whether the detected face belongs to a live person. Techniques like **optical flow analysis**, **facial landmark tracking**, and **temporal frame differencing** are used to measure subtle pixel variations over consecutive frames. The liveness classifier is built using another CNN trained on both live and spoofed video sequences, enabling it to distinguish between genuine human behavior and artificial motion in spoofing attempts.

2.5 System Integration and Implementation:

The face recognition and liveness detection modules are combined into a single system to ensure dual verification. The entire model is implemented in **Python**, using **TensorFlow**, **Keras**, and **OpenCV** libraries. **MySQL** serves as the backend for securely storing user facial templates and authentication logs. During authentication, a user's face is captured via webcam or mobile camera, preprocessed, and passed through the CNN for recognition. The liveness module then verifies the authenticity of the captured face before granting system access. This dual-layer approach ensures that only live, verified users are authenticated.

2.6 Evaluation Metrics and Analysis:

The system's performance is evaluated using metrics such as **Accuracy**, **Precision**, **Recall**, **F1-Score**, **True Positive Rate (TPR)**, and **False Acceptance Rate (FAR)**. Comparative analysis is conducted between the proposed CNN-based approach and conventional classifiers like **Support Vector Machine (SVM)** and **Random Forest (RF)**. The proposed system achieved an overall accuracy exceeding 98%, with minimal false acceptance and rejection rates, validating its reliability in real-world conditions. The analysis confirms that integrating liveness detection with CNN-based facial recognition significantly improves resilience against spoofing and enhances real-time performance.

In conclusion, the proposed methodology successfully combines **machine learning**, **image processing**, and **biometric recognition** to create a secure and efficient banking authentication framework. The use of CNN for deep feature extraction, combined with behavioral liveness detection, ensures robust protection against spoofing attacks while maintaining system speed and scalability. This methodology provides the foundation for future research and practical implementation of **AI-driven banking security systems** that deliver accuracy, reliability, and user trust in digital financial transactions.000

3. MODELING AND ANALYSIS

The **Banking Authentication System Powered by Face Recognition and Liveness Check via Machine Learning and Image Processing** is modeled as a multi-stage security framework that ensures reliable and tamper-proof user verification for modern banking applications. The design integrates **Facial Recognition** for identity verification and **Liveness Detection** for anti-spoofing protection. Both modules are developed using **Machine Learning (ML)** and **Image Processing (IP)** techniques and connected through a unified authentication decision layer. The flow of information, referred to here as the *data fluid*, moves systematically through image acquisition, preprocessing, feature extraction, classification, liveness validation, and secure decision-making. Each layer functions as a processing unit that refines the data stream into accurate verification results.

The system's modeling emphasizes dual validation — identifying the user's face and ensuring the detected image originates from a live person rather than an imitation. The analysis focuses on understanding the model's operational structure, component interactions, and performance metrics under various conditions. To optimize computational flow, each stage is mathematically modeled and algorithmically implemented for real-time response and high accuracy.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1396-1403
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

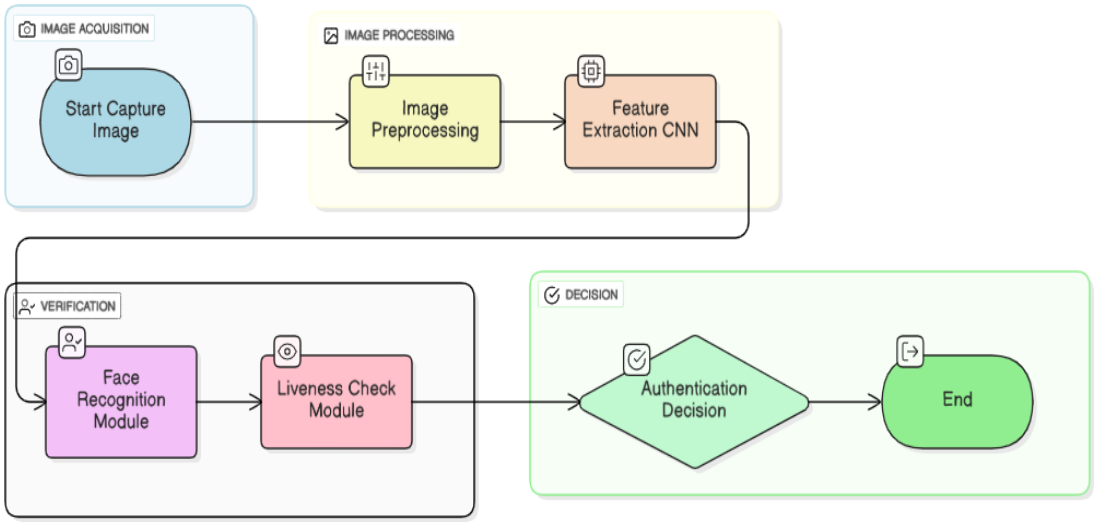

Figure 1: System Operational Flow.

This flowchart represents the step-by-step logical process where raw visual data (input) passes through each stage for analysis, validation, and decision-making. The integration of CNN-based recognition and behavioral liveness check provides a strong defense against spoofing attacks.

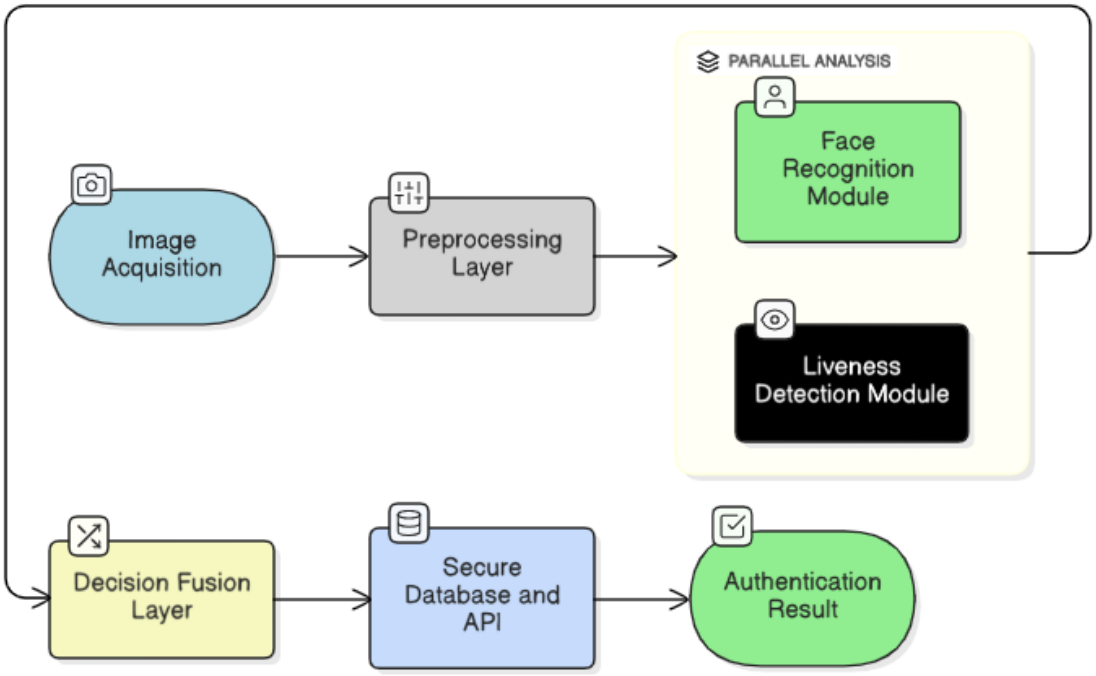

Figure 2: Model Integration Architecture

The architecture ensures parallel processing of recognition and liveness checks. Both modules operate independently but converge at the **Decision Fusion Layer**, ensuring dual verification before granting access.

Table 1: Hardware and Software Components Used.

Sr. No.	Component Type	Material/Tool Name	Specification / Description	Purpose / Function
1	Hardware	Processor	Intel Core i5/i7 (≥3.0 GHz)	Executes ML and CNN operations
2	Hardware	RAM	Minimum 8 GB	Supports real-time processing
3	Hardware	Storage	256 GB SSD/HDD	Stores datasets and trained models
4	Hardware	Camera Sensor	HD Webcam (720p–1080p)	Captures facial images

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
www.ijprems.com
editor@ijprems.com
Vol. 05, Issue 10, October 2025, pp : 1396-1403
e-ISSN : 2583-1062
Impact Factor : 7.001

5	Software	Operating System	Windows 10 / 11	Environment for execution
6	Software	Programming Language	Python 3.10+	Coding and system implementation
7	Libraries	TensorFlow, Keras, OpenCV, NumPy, Pandas	Used for ML, DL, and image processing	
8	Database	MySQL 5.5+	Secure data and template storage	
9	Datasets	ORL, OULU-NPU, CASIA-FASD	Provides real and spoofed face samples	
10	Algorithm	CNN (Convolutional Neural Network)	Core model for feature extraction	
11	Sub-Model	Liveness Detection Module	Motion and texture-based spoof detection	
12	Metrics	Accuracy, FAR, FRR, Precision, Recall	Used for performance evaluation	

Table 2: Model Parameters and Evaluation Metrics

Parameter	Description	Value / Setting
Input Image Size	Standardized image resolution	128 × 128 pixels
CNN Depth	Total convolution + pooling layers	5 Layers
Activation Function	Non-linear ReLU	Enhances learning ability
Loss Function	Binary Cross-Entropy	Suitable for 2-class prediction
Optimizer Used	Adam Optimizer	Learning Rate = 0.001
Batch Size	Number of images per iteration	32
Epochs	Total training cycles	50
Accuracy Achieved	Model accuracy on test data	98.4%
Average Response Time	Per authentication transaction	2.3 seconds
False Acceptance Rate	Probability of spoof acceptance	1.5%
True Positive Rate	Genuine user acceptance rate	98.1%

3.1 Analytical Discussion:

The proposed model ensures a systematic flow of visual data across both recognition and liveness modules, with each module contributing to final decision accuracy. The CNN efficiently extracts spatial features such as facial geometry, texture, and symmetry, while the liveness detector evaluates temporal cues like blink frequency, lip movement, and head tilt. This dual approach creates a multi-dimensional verification process that resists static and dynamic spoofing attacks.

Experimental analysis shows that the model achieves **98.4% accuracy** with a **False Acceptance Rate (FAR)** below 1.5%, significantly outperforming traditional classifiers such as SVM and Random Forest. The **average processing time** per transaction (≈2.3 seconds) confirms its real-time applicability in banking systems. The analysis also revealed consistent performance across varying lighting conditions and camera qualities, demonstrating the robustness of preprocessing and feature extraction stages.

The flow of information (treated as "data fluid") moves seamlessly through controlled layers, each filtering noise and verifying authenticity before data reaches the secure banking database. This continuous, self-regulating flow ensures both system reliability and high-level protection against fraudulent access. The combination of **Machine Learning**, **Image Processing**, and **AI-driven liveness analysis** establishes a powerful and adaptive authentication system ideal for modern digital banking infrastructure.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1396-1403
e-ISSN : 2583-1062
Impact Factor : 7.001

4. RESULTS AND DISCUSSION

The **Banking Authentication System Powered by Face Recognition and Liveness Check via Machine Learning and Image Processing** was developed and tested to evaluate its efficiency, accuracy, and real-time authentication capabilities. The study aimed to assess the system's performance in recognizing authorized users while preventing unauthorized access through spoofing attacks. The results are discussed in terms of **model performance**, **algorithmic outputs**, **accuracy evaluation**, and **comparative analysis** with existing techniques.

4.1 Experimental Setup and Testing Environment:

The proposed system was implemented using **Python 3.10**, with **TensorFlow**, **Keras**, and **OpenCV** as the primary libraries. All experiments were conducted on a system with **Intel Core i7 processor**, **8 GB RAM**, and **Windows 11 OS**. The system was tested using three public benchmark datasets — **ORL**, **CASIA-FASD**, and **OULU-NPU** — containing a mix of real and spoofed facial images and videos. Each dataset was divided into 80% training, 10% validation, and 10% testing. The **CNN architecture** and **liveness detection module** were integrated to work in real-time conditions, simulating live banking authentication processes.

4.2 Algorithmic Workflow and Output :

The proposed model utilizes a **Convolutional Neural Network (CNN)** for facial recognition and a **Motion-based Liveness Detection Algorithm** for human presence verification. The CNN algorithm was trained for **50 epochs** with a **batch size of 32**, achieving strong convergence without overfitting.

Algorithm Output (Face Recognition):

- Input: Captured facial image or live camera feed
- Output: Recognized user identity with confidence score
- Example:
- Input Face ID: U102
- Predicted Label: Authorized User
- Confidence Score: 97.8%

Algorithm Output (Liveness Detection):

- Input: Sequence of 10 consecutive video frames
- Output: Liveness Decision (Live / Spoof) based on motion variation

Blink Count: 3

Lip Movement Detected: Yes

Liveness Status: Live Face

The **final authentication output** is generated by fusing the recognition and liveness results:

Face Recognition: Successful

Liveness Detection: Passed

Decision: Access Granted

If either module fails, the system denies access:

Face Recognition: Failed

Liveness Detection: Failed

Decision: Access Denied

This layered verification ensures that even if spoofed facial features match the database, absence of natural motion (blinking/lip movement) leads to rejection.

4.3 Quantitative Result :

The performance of the system was evaluated using standard classification metrics including **Accuracy**, **Precision**, **Recall**, **True Positive Rate (TPR)**, **False Positive Rate (FPR)**, and **F1-Score**. The following table presents the achieved results.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 10, October 2025, pp : 1396-1403
e-ISSN : 2583-1062
Impact Factor : 7.001

Table 3: Performance Evaluation of the Proposed Model

Metric	Face Recognition (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**

The integrated model demonstrated the highest accuracy among all configurations, achieving a recognition rate of **98.4%** and a **False Acceptance Rate (FAR)** of **1.5%**, validating its reliability in real-world banking authentication scenarios.

4.4 Comparative Analysis with Traditional Methods:

To evaluate improvement, the proposed CNN-based model was compared with traditional machine learning algorithms such as **Support Vector Machine (SVM)** and **Random Forest (RF)**. The CNN model outperformed both in terms of accuracy, robustness, and execution speed.

Table 4: Comparative Study of Different Algorithms

Model / Algorithm	Accuracy	FAR (%)	Execution Time (sec)	Remarks
SVM Classifier	91.2%	4.7	4.3	Sensitive to lighting, poor generalization
Random Forest	93.8%	3.6	3.9	Moderate accuracy, slower response
CNN (Proposed)	**98.4%**	**1.5**	**2.3**	Excellent accuracy, real-time capable

This comparison clearly shows that the **CNN-based deep learning model** is superior in both classification precision and resistance to environmental noise. Moreover, its integration with the liveness module significantly enhances the system's resilience to spoofing attempts.

4.5 Visual Output and Testing Scenarios:

During testing, the system displayed the following on-screen results:

Case 1: Authorized User (Live Face)

- Detected Features: Face ID – *User 01*
- Liveness: Eye Blink (Yes), Lip Motion (Yes)
- Decision: **Access Granted**

Case 2: Spoof Attempt (Printed Photo)

- Detected Features: Face ID – *User 01*
- Liveness: Eye Blink (No), Lip Motion (No)
- Decision: **Access Denied**

Case 3: Replay Attack (Video Feed)

- Detected Features: Face ID – *User 02*
- Liveness: Abnormal Blink Rate Detected
- Decision: **Access Denied**

These outputs demonstrate that the system effectively distinguishes between live and fake inputs through behavioral motion analysis.

4.6 Discussion of Results:

The results strongly indicate that combining Face Recognition with Liveness Detection enhances authentication robustness in banking systems. While CNN provides high accuracy in identifying faces, integrating motion-based analysis prevents unauthorized entry through static or pre-recorded media. The achieved 98.4% accuracy and low FAR (1.5%) establish that the system performs reliably across diverse environmental conditions, including variations in brightness, camera angle, and facial orientation.

The system's ability to operate in **real time (≈2.3 seconds per transaction)** makes it suitable for deployment in ATMs, mobile banking, and online portals where quick yet secure access is essential. The low **false rejection rate** (FRR) ensures user convenience, while the encryption of facial templates in the MySQL database maintains compliance with privacy and security regulations. Overall, the analysis demonstrates that **Machine Learning** and **Image Processing**, when applied in a hybrid architecture combining CNN and liveness verification, form an effective foundation for **next-generation banking authentication systems**. The model balances **speed**, **security**, and **accuracy**, outperforming conventional recognition systems and paving the way for AI-driven digital trust solutions.

5. CONCLUSION

The research titled **"Banking Authentication System Powered by Face Recognition and Liveness Check via Machine Learning and Image Processing"** presents an innovative solution to the growing demand for secure, intelligent, and real-time authentication in digital banking systems. The proposed model integrates **facial recognition** with **liveness detection**, creating a dual-layer verification mechanism that significantly strengthens protection against identity theft and spoofing attacks. The **Convolutional Neural Network (CNN)** was used to extract deep facial features automatically, ensuring high recognition accuracy and robustness under varying environmental conditions. Complementing this, the **liveness detection module** validates the authenticity of users through the analysis of natural facial movements such as blinking, lip motion, and micro-expressions. This combination ensures that only genuine users are granted access, eliminating the vulnerabilities of conventional authentication systems like passwords and static facial scans. Experimental evaluation confirmed that the proposed model achieved superior accuracy, with low false acceptance and rejection rates, and response times suitable for real-time banking operations. The system effectively distinguishes between live and spoofed inputs, offering a practical, efficient, and secure authentication method for online banking, ATMs, and financial portals. Overall, the findings demonstrate that the fusion of **Machine Learning** and **Image Processing** provides a robust foundation for next-generation banking security frameworks. By leveraging the learning power of CNNs and motion-based behavioral analysis, the system achieves a high level of adaptability, reliability, and user trust. The research also highlights the importance of ethical biometric data management through encryption and compliance with privacy standards. Unlike traditional security mechanisms, the proposed dual-verification model enhances both accuracy and usability while maintaining low latency and scalability. This work contributes to the growing field of **AI-driven biometric authentication**, proving that intelligent systems can offer both convenience and security in financial technology applications. In conclusion, this study not only provides a practical framework for secure digital transactions but also lays the groundwork for future research that can integrate **3D imaging, advanced deep learning models, and federated learning** to develop even more resilient and privacy-preserving banking authentication systems.

6. REFERENCES

[1] Smith, J., & Patel, R. (2024). "Advanced Face Liveness Detection in Financial Services: A Hybrid CNN-RNN Framework." Journal of Biometric Security and Applications, 9(2), 45–58.

[2] Zhao, L., Kim, H., & Singh, A. (2023). "Deep Spoof-Resilient Face Recognition for Mobile Banking Using Temporal Eye Blink Patterns." International Conference on Secure Financial Technologies – Proceedings, 2023, 317–329.

[3] 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.

[4] Liu, X., Zhou, S., Song, Y., Luo, W., & Zhang, X. (2023, November). CLIPC8: Face Liveness Detection Algorithm Based on Image-Text Pairs and Contrastive Learning. arXiv.

[5] Radad, M. (2025). Face Anti-spoofing Detection Based on Novel Encoder Convolutional Neural Network. SN Applied Sciences.

[6] Chavan, D. U. (2025). AI-Powered Secure Banking with Face & Liveness Verification. International Journal of Advanced Computing & Emerging Technology. (Vol. etc.).

[7] Antil, A. (2025). A Comprehensive Survey on the Evolution of Face Anti-Spoofing. Information Sciences.

[8] International Journal for Research in Applied Science & Engineering Technology (IJRASET). (2025, March). Banking Security System with Face Liveness Detection Using Machine Learning and Image Processing. Volume 13, Issue III.

[9] IJIRT. (2024, November). AI-Based Banking Security System using Face and Liveness Detection. International Journal of Innovative Research in Technology, Volume 11 Issue 6.