*Journal of Computer Science*

Research Paper

# Enhancing E-Banking Security and Personalization through Convolutional Neural Network-Based Facial Recognition

**Ramy Kamal Amin[1], Ghada A. El Khayat[1], Farid El Sahn[2], Abeer A. Amer[1,3]**

[1] *Department of Information Systems and Computers, Faculty of Business, Alexandria, Egypt*
[2] *Department of Business Administration, Faculty of Business, Alexandria, Egypt*
[3] *Department of Computer Science and Information Systems, Faculty of Management Sciences, Sadat Academy for Management Sciences, Egypt*

*Article history*
Received: 27-02-2025
Revised: 26-04-2025
Accepted: 09-05-2025

*Corresponding Author:
Ramy Kamal Amin,
Department of Information Systems and Computers, Faculty of Business, Alexandria, Egypt
Email: ramy.kamal@eia.edu.eg

**Abstract:** Facial recognition technology has become a cornerstone in enhancing the security and user experience of electronic banking services. Its ability to provide a seamless yet secure authentication method is vital in combating fraud and maintaining the integrity of online financial transactions. This study presents the development of an advanced electronic banking system that strengthens security through the integration of a Convolutional Neural Network (CNN)–based facial recognition model. The system combines facial recognition with One-Time Password (OTP) verification to provide multi-factor authentication. The proposed system includes a web-based user interface and is trained to distinguish between genuine and fraudulent facial recognition attempts. The training dataset consists of 26 genuine and 26 fraudulent videos, from which 150 frames were extracted per video, yielding a total of 7,800 frames. The dataset was divided into 80% for training and 20% for testing. The CNN model achieved an accuracy of 99.92% in differentiating between real and spoofed facial images, demonstrating strong capability in detecting attempts to deceive the system. This high accuracy highlights the model's robustness and reliability in securing electronic banking services, significantly enhancing the safety and integrity of online financial transactions. The integration of OTP verification provides an additional security layer, ensuring that even if facial recognition were compromised, unauthorized access would still be prevented. Overall, the results emphasize the potential of deep learning techniques and multi-factor authentication in strengthening cybersecurity measures within the banking sector.

**Keywords:** Facial Recognition, Artificial Intelligence (AI), Deep Learning (DL), Anti-Spoofing, CNN Algorithm, User Experience, Liveness Detection.

## Introduction

Facial authentication, offering a straightforward yet highly effective approach to identification and recognition on mobile devices, has become increasingly prevalent in applications such as phone unlocking, app logins, and online payment systems. According to a market analysis report (Facial Recognition Market Size & Share Analysis – Growth Trends & Forecasts (2025–2030), 2025), the facial recognition market is projected to grow substantially, reaching an estimated value of USD 16.27 billion by 2030.

Studies have shown that facial authentication systems remain vulnerable to a range of security threats (Yan and Yang, 2023), primarily due to inherent weaknesses in the deep learning algorithms used within these systems. Such vulnerabilities can be exploited through carefully crafted adversarial examples (Byun et al., 2022). Furthermore, the widespread use of social networking platforms, such as Facebook, has made it easier for attackers to obtain facial images or videos of individuals and construct counterfeit facial models (Wang et al., 2023). Attackers can employ media-based facial forgery (MFF) techniques to impersonate a target's facial features using advanced algorithms and high-resolution printers or screens (Tan et al., 2021).

The rapid advancement of technology and the increasing reliance on digital platforms have also transformed how banking services are accessed and delivered. However, this digital shift brings new challenges, particularly regarding security. Protecting sensitive customer information and preventing unauthorized access or fraudulent activities have become critical concerns for the banking sector. Traditional authentication methods such as passwords and Personal Identification Numbers (PINs) have proven vulnerable to multiple forms of attack (Pawar and Rokade, 2023). These mechanisms lack the capability to differentiate between legitimate users and impostors who gain illicit access using stolen credentials (Khairnar et al., 2023).

Additionally, users often forget passwords or PINs, and access cards can be misplaced or lost. Biometric systems offer an effective alternative by enabling automated identification without the need to memorize or carry authentication tokens. Biometric authentication provides a user-friendly and efficient solution (Venkata et al., 2020).

Facial recognition, one of the most widely used biometric technologies, offers diverse applications across numerous fields. It is expected that large international companies will continue adopting biometric authentication for access control and fraud prevention. However, one of the most significant challenges facing biometric recognition systems is deceptive identification, commonly known as spoofing attacks. Facial artifacts belonging to an authorized user can be fabricated using photographs or video footage obtained from publicly accessible social media platforms. An impostor can exploit such vulnerabilities to gain unauthorized access to facial recognition systems lacking robust protective measures (Ming et al., 2020). Consequently, there is a growing need for strong security systems capable of providing reliable and convenient authentication while mitigating identity theft and unauthorized access risks (Hangaragi et al., 2023).

To address this challenge, liveness detection techniques have been introduced. Liveness detection aims to verify that a real person is physically present in front of the camera, ensuring that authentication is not performed using spoofed images or videos. These techniques analyze facial cues and subtle movements characteristic of a living individual (Machap and Marco, 2023).

## Literature Review

Face recognition and liveness detection play crucial roles in enhancing the security of e-banking systems, safeguarding against unauthorized access and fraudulent activities. Recent literature has extensively investigated various techniques and methodologies to improve the accuracy and robustness of these biometric authentication systems. Face recognition algorithms—including deep learning-based approaches such as Convolutional Neural Networks (CNNs) and feature-based methods like Local Binary Patterns (LBP)—have been widely explored for their effectiveness in identifying users based on facial features.

Liveness detection mechanisms have also gained considerable attention as a means to prevent spoofing attacks, in which adversaries attempt to deceive the system using fake images or videos. Techniques such as texture analysis, motion detection, and 3D depth sensing have been integrated into e-banking systems to ensure the presence of a live user during authentication. Despite significant advancements, challenges such as illumination variations, occlusions, and adversarial attacks remain active areas of research. Future efforts in this domain aim to develop robust and reliable solutions that strengthen the security of e-banking platforms and enhance user experience.

This review is divided into three sections: the first discusses the importance of biometric authentication in e-banking, the second illustrates face recognition technologies, and the third examines studies related to liveness detection and anti-spoofing techniques.

### *The Importance of Biometric Authentication in E-Banking*

Alkaseasbeh et al. (2024) explored how biometric authentication features—including unique biological traits, multifactor authentication, non-replicability, continuous authentication, and anti-spoofing measures—enhance financial service security in FinTech. Their findings revealed that biometric authentication significantly improves security, with anti-spoofing techniques effectively preventing hacking and unauthorized access. The study emphasized the need for greater awareness of authentication's importance while also acknowledging potential vulnerabilities.

Alorfi et al. (2023) highlighted that biometrics and FinTech are rapidly advancing technologies. Traditional banks integrate FinTech into online banking and mobile payments, while FinTech-based banks operate fully digitally. Biometrics enhance security in financial services and provide a competitive edge, helping companies retain their customers.

Ali (2022) noted that FinTech—supported by affordable high-speed internet and advanced smartphones—has transformed financial services, including banking, payments, and wealth management. However, existing mobile money systems relying on PIN and SIM authentication face security challenges due to short PINs, lack of expiration, and unmasked entry, underscoring the need for stronger authentication methods.

Xu (2022) reported that biometrics, initially used in law enforcement, is now widely applied in financial services such as e-banking and online payments. The COVID-19 pandemic accelerated the adoption of contactless biometric solutions. The biometrics market, valued at USD 24.1 billion in 2020, is projected to grow to USD 82.8 billion by 2027, with mobile biometrics expected to reach USD 79.8 billion, reflecting rapid global integration.

Gomaa et al. (2022) emphasized that anti-spoofing measures represent a key advancement in FinTech authentication, effectively preventing impersonation using biometric standards. However, spoofing attacks using fabricated biometric samples remain a threat, indicating the need for stronger countermeasures.

Indrasari et al. (2022) analyzed e-banking user satisfaction and loyalty during COVID-19, focusing on service quality factors such as reliability, privacy, security, design, and customer service. Results showed that privacy and security significantly influence user loyalty, reinforcing their importance in digital banking environments.

Afroze et al. (2021) similarly stressed that privacy and security are essential in e-banking to ensure user trust, secure transactions, and long-term customer confidence.

### *Face Recognition Technologies*

Jameil and Hassan (2023) introduced a two-level authentication system for internet banking, combining PIN or fingerprint login at the first level. Using PCA and eigenface techniques with an SVM classifier, their model achieved a 92% recognition rate, improving security and user experience.

Hangaragi et al. (2023) proposed a face detection and recognition model using Face Mesh capable of handling diverse conditions such as varying lighting and backgrounds. Trained on the LWF dataset and real-time images, it processed non-frontal images across age, gender, and race, achieving 94.23% accuracy and demonstrating robust performance.

Jabberi et al. (2023) presented a deep learning-based 3D face recognition method using 3D CNNs such as 3D ShapeNets. Their model achieved recognition accuracies of 94.25%, 97.9%, and 98.31% on the LFPW, BU3DFE, and FRAV3D datasets, respectively, outperforming 2D methods. The study highlighted the superiority of 3D recognition and recommended exploring additional 3D CNN architectures.

Kumar et al. (2023) focused on identifying four emotions (anger, sadness, neutral, and happiness) from Manipuri speech clips using a deep CNN model. The model employed MFCC for speech feature extraction and aimed to improve emotion prediction accuracy through combined speech and facial analysis.

Sam et al. (2022) proposed a secure banking system using a DCNN algorithm for face authentication coupled with cloud-based OTP codes, eliminating the need for debit cards at ATMs. This solution reduces fraud risks such as skimming and jackpotting, while offering greater convenience for cardless transactions.

Kalmani and Dilna (2022) proposed a facial recognition-based ATM security solution that verifies users' real-time images against stored data, effectively using the face as a password. Their research addressed card theft and duplication issues and explored machine learning implementation on embedded hardware.

### *Liveness Detection and Anti-Spoofing Techniques*

Surantha and Sugijakko (2024) developed a lightweight liveness detection system using MobileNetV2 on a Raspberry Pi. Their model achieved 96% accuracy for live subjects and successfully detected spoof attacks with 79–83.7% accuracy, processing each sample in under 0.6 seconds.

Basurah et al. (2023) implemented a liveness detection system using facial movements with TensorFlow.js and face-api.js, achieving 85% accuracy for face recognition and 82.5% for expression detection. To counter video spoofing, an object detection system using ml5.js was integrated, with results showing face-api.js outperforming GLCM-based methods.

Khairnar et al. (2023) conducted a PRISMA-based systematic review of face-liveness detection research from the past decade, covering spoofing attacks, feature extraction methods, and AI approaches including machine learning and deep learning. The review also explored emerging topics such as Explainable AI, Federated Learning, Transfer Learning, and Meta-Learning.

Widjaya and Wicaksana (2023) introduced a randomized challenge-response approach for liveness detection, requiring users to perform actions such as blinking or head movements. Their method achieved 99% accuracy and a 98.99% F-score, effectively mitigating photo and video spoofing attacks.

Wei et al. (2022) proposed an optimized LeNet-5 model for liveness detection, achieving a 99.9% recognition rate. By increasing convolution kernel size and incorporating global average pooling, their model outperformed SVM (96.67%) and standard LeNet-5 (98.23%).

Venkata et al. (2020) addressed spoofing as a major threat to facial recognition systems, reviewing attacks such as mask, photo, and video spoofing. They evaluated detection methods including LBP, DMD, SVM, CNN, and hybrid techniques, demonstrating their effectiveness in improving biometric security.

## Proposed Solution

### *The Survey*

A comprehensive survey was conducted to evaluate the effectiveness and relevance of integrating face recognition with anti-spoofing measures in e-banking applications. It aimed to assess users' perceptions of the importance of biometric security features and identify key factors they value in a secure yet user-friendly platform. The survey explored attitudes toward the effectiveness of these technologies in enhancing security, usability factors like ease of access and speed, and the balance between security and convenience. It also examined user priorities, such as accuracy, reliability, and handling errors like false rejections. The findings provide actionable insights for developers and financial institutions to design user-centered systems that align with customer expectations, ensuring high satisfaction and trust.

### *Survey Design*

The survey employs snowball sampling to reach Egyptian nationals as potential e-banking users, leveraging initial respondents to expand participation via referrals. Designed in Arabic for clarity and cultural relevance, the survey includes ten mandatory closed-ended questions assessing perceptions of face recognition and anti-spoofing in e-banking, plus an optional open-ended question for qualitative feedback. A target sample of 200 respondents ensures diverse insights, with Google Forms used for easy data collection. Distributed via Facebook and WhatsApp, the survey taps into popular platforms to maximize reach. This approach aims to gather actionable data on user preferences, security concerns, and design priorities to inform the development of user-centric biometric systems in e-banking.

### *The Survey Questions Translated in English Language*

- *Closed-ended Questions*

1. Do you have a bank account?
2. Do you use electronic banking services?
3. To what extent are you satisfied with the idea of using facial recognition technology to enhance the login process for electronic banking applications?
4. What are your main concerns regarding the use of facial recognition technology in electronic banking applications?
5. Do you believe that using facial recognition technology will make electronic banking services faster and more secure?
6. Do you have any reservations about sharing your picture with the bank for security purposes?
7. How easy is it for you to use facial recognition technology when logging into electronic banking applications?
8. What duration do you think would be acceptable to complete the facial recognition process?
9. What is your level of confidence in the ability of facial recognition technology to prevent fraud and identity theft?
10. Would you prefer increased security requirements by using facial recognition technology along with traditional methods like passwords?

- *Open-ended Question*

11. Do you have any suggestions or additional comments on improving customer experience using facial recognition technology?

### *Survey Results*

A survey of 200 e-banking users highlights strong support for integrating facial recognition technology, with 79% expressing satisfaction with the idea and 66.3% believing it will enhance speed and security. Privacy (38.5%) and security (39.5%) emerge as primary concerns, emphasizing the need for robust safeguards. While 74% are willing to share photos for the system, 70.5% favor combining facial recognition with password-based authentication for added protection. Most respondents expect authentication within 5–10 seconds and trust the technology to prevent fraud (65.5%). Concerns about spoofing attacks are addressed through advanced anti-spoofing measures. These insights guide a user-centered design focused on efficiency, security, and trust.

### *System Testing*

The system testing experiment consists of two main phases, each designed to rigorously evaluate four critical components essential to the system's successful development and implementation: accuracy, speed, privacy, and security. These elements are vital in ensuring that the system not only performs reliably but also meets the expectations and needs of its users while safeguarding their personal information.

- *Phase One*

In the first phase, an exploratory pilot test was conducted involving 150 banking customers to evaluate a prototype version of the proposed system. This preliminary testing aimed to assess the system's performance in terms of accuracy, speed, privacy, and security under real-use conditions. Participants' interactions with the system were closely monitored, and their feedback was collected through a structured follow-up survey. The insights gathered from this phase were critical in identifying areas for improvement and refining the system's functionality. This iterative process ensured that the proposed system was optimized and ready for subsequent large-scale implementation.

- *Phase Two*

In the second phase, the refined system was subjected to comprehensive testing with an expanded and diverse client base of 500 users in a controlled environment designed to simulate real-life banking scenarios. This large-scale evaluation aimed to assess the system's performance across critical metrics, including accuracy, speed, privacy, and security. The testing environment was carefully selected to replicate the operational conditions of a banking setting, ensuring that the system could reliably and swiftly authenticate users while maintaining the highest standards of data protection. Detailed user feedback was systematically collected, with a particular focus on perceptions of privacy and security, to identify areas for improvement. This feedback was instrumental in making final adjustments to the system, enhancing both its functionality and user experience. The results confirmed that the system meets rigorous technical and user-centered standards, delivering a secure, efficient, and seamless biometric authentication solution tailored for e-banking applications.

### *Ensuring Privacy and Compliance*

The developed facial recognition and anti-spoofing system is fully compliant with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). It employs an SQL database to securely store encrypted user data (limited to essential personal details and profile images) for authentication purposes. The system ensures compliance by obtaining explicit user consent, adhering to data minimization principles, and transparently informing users about data collection purposes. Users can access, update, or delete their data by notifying the system administrator, fulfilling GDPR and CCPA rights. Robust security protocols protect sensitive information, aligning with legal standards to safeguard privacy, ensure compliance, and build trust.

## System Implementation and Results

The proposed phases explained in Fig. 1 outline a comprehensive framework for a secure facial recognition system. The image highlights key components, including Face Capture, Face Detection, Face Recognition, Liveness Detection, and OTP Authentication. These elements collectively ensure a robust and multi-layered approach to identity verification. Face Capture and Detection initiate the process by identifying and isolating facial features, while Face Recognition matches these features against stored data. Liveness Detection adds an essential security layer by distinguishing between real users and spoofed attempts, such as photographs or videos. Finally, OTP (One-Time Password) Authentication provides an additional verification step, enhancing the system's overall security. This framework exemplifies a modern, secure, and efficient approach to biometric authentication, addressing both accuracy and anti-spoofing challenges.

Using PyCharm and the Python programming language, a deep learning model was developed and trained to distinguish between genuine and fraudulent facial recognition attempts. The training dataset comprises 26 genuine and 26 fraudulent videos, with 150 frames extracted from each video, resulting in a total of 7,800 frames. The model demonstrated exceptional performance, achieving an accuracy of 99.92% in recognizing individuals and detecting spoofing attempts. To simulate a banking application and enable user testing, the model was integrated with a web-based user interface developed using HTML, CSS, and JavaScript. The Python code implements a Flask-based secure banking system that integrates face recognition and anti-spoofing technologies. It employs a convolutional neural network (CNN) to detect spoofing attempts, trained with synthetic face data and adversarial samples to effectively distinguish between genuine and fake faces.

The DeepFace library, utilizing a pre-trained VGG-Face model with a cosine distance metric, is used for face recognition. This system processes face images in real-time, detects and extracts facial regions, and verifies them against a stored dataset. Additional security is ensured through OTP verification and cross-validation of user data. The dataset includes user-uploaded face images stored locally, which are dynamically compared during login or registration. This multi-layered approach combines real-time CNN anti-spoofing with deep learning-based face verification to enhance security in banking operations, providing a robust solution for fraud detection and user authentication.

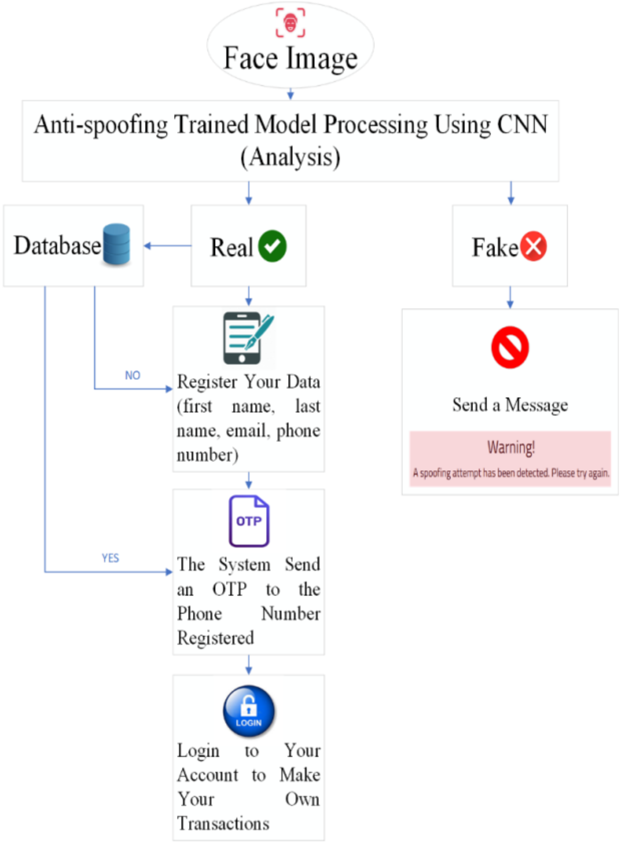

Face Image
Anti-spoofing Trained Model Processing Using CNN (Analysis)
Database
Real
Fake
NO
YES
Register Your Data (first name, last name, email, phone number)
OTP
The System Send an OTP to the Phone Number Registered
LOGIN
Login to Your Account to Make Your Own Transactions
Send a Message
Warning!
A spoofing attempt has been detected. Please try again.

**Fig. 1:** Proposed Phases

## Model and System Steps

### *Data Collection and Preprocessing*

Dataset Collection: A dataset comprising both real and fake (spoofed) images and videos is collected. The dataset is organized into separate folders for real and fake samples to facilitate supervised learning. Image Preprocessing: All images and video frames are resized to a fixed resolution (e.g., 160x160 pixels). Pixel values are normalized to the range [0, 1] by dividing by 255 to ensure consistency in input data.

Video Frame Extraction: Frames are extracted from videos at fixed intervals or up to a maximum number of frames (e.g., 150 frames per video). Each frame is treated as an individual image for training purposes.

### *Model Architecture Design*

Convolutional Neural Network model is designed with the following layers:

- Input Layer: Accepts images of size 160x160x3 (height, width, channels).
- Convolutional Layers: Three convolutional layers with 32, 64, and 128 filters, respectively. Each layer uses a 3x3 kernel, ReLU activation, and L2 regularization to mitigate overfitting.
- Max Pooling Layers: Applied after each convolutional layer to reduce spatial dimensions.
- Flatten Layer: Converts the 3D output of the convolutional layers into a 1D feature vector.
- Fully Connected Layers: A dense layer with 128 units and ReLU activation, followed by a dropout layer (dropout rate = 0.5) to further prevent overfitting.
- Output Layer: A single unit with a sigmoid activation function to classify the input as real (1) or fake (0).

### *Model Compilation*

- Optimizer: The Adam optimizer is used with a learning rate of 0.001.
- Loss Function: Binary cross-entropy is employed as the loss function, suitable for binary classification tasks.
- Metrics: Accuracy is used as the primary evaluation metric.

### *Data Augmentation*

Data augmentation techniques are applied to enhance the diversity of the training data and improve model generalization. Techniques include:

- Rotation (up to 20 degrees).
- Width and height shifting (up to 20% of the image size).
- Shearing and zooming (up to 20%).
- Horizontal flipping.
- Nearest fill mode for padding.

### *Model Training*

- Training-Validation Split: The dataset is split into training (80%) and validation (20%) sets.
- Batch Training: The model is trained using mini-batches (e.g., batch size = 16) to optimize memory usage and computational efficiency.
- Early Stopping: Early stopping is implemented to halt training if the validation loss does not improve for 5 consecutive epochs, preventing overfitting and saving the best model weights.
- Epochs: The model is trained for up to 50 epochs or until early stopping is triggered.

### *Model Evaluation*

- Performance Metrics: The model is evaluated on the test set using the following metrics:
- Accuracy: Percentage of correctly classified samples.
- Precision: Proportion of true positives among all predicted positives.
- Recall: Proportion of true positives among all actual positives.

- F1 Score: Harmonic mean of precision and recall.
- Confusion Matrix: A confusion matrix is used to visualize the distribution of true positives, true negatives, false positives, and false negatives.
- Classification Report: A detailed classification report is generated, summarizing precision, recall, F1 score, and support for each class.

### *Model Saving*

The trained model is saved to a file (e.g., anti_spoofing_model.h5) for future use in real-time applications.

### *Real-Time Prediction*

Image Preprocessing: For real-time predictions, input images are preprocessed by resizing them to 160x160 pixels and normalizing pixel values.

Prediction: The trained model is used to predict whether the input image is real or fake. A prediction value greater than 0.5 is classified as real, and less than or equal to 0.5 is classified as fake.

### *Visualization of Training Progress*

Training and validation accuracy and loss curves are plotted to monitor the model's learning progress and detect overfitting or underfitting.

### *Model Deployment*

The trained model is integrated into a Flask-based web application to provide real-time anti-spoofing predictions via an API.

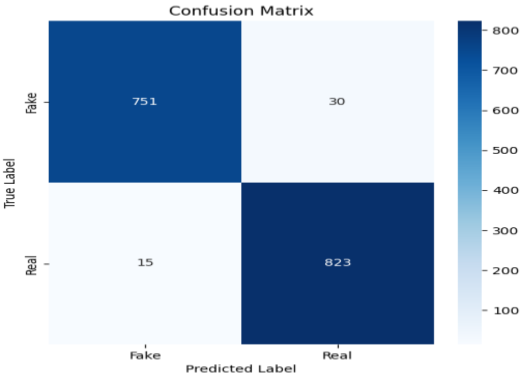


**Fig. 2:** Confusion Matrix

### *Model Assessment*

The confusion matrix illustrates the performance of face recognition and anti-spoofing system in distinguishing between real and fake images. Fig. 2 demonstrates the matrix consists of four values: 751 true positives (correctly identified fake images), 823 true negatives (correctly identified real images), 30 false negatives (fake images misclassified as real), and 15 false positives (real images misclassified as fake). The low number of misclassifications indicates a high level of accuracy and robustness in detecting spoofing attempts while minimizing false rejections of genuine users.

The graphs in Fig. 3 illustrate the training and validation accuracy (left) and loss (right) over multiple epochs for a face recognition and anti-spoofing model. The accuracy plot demonstrates a steady increase in training accuracy, with validation accuracy exhibiting fluctuations but generally maintaining higher values, suggesting effective generalization. The loss plot indicates a consistent decline in both training and validation loss, with validation loss showing greater variability. The convergence of training and validation metrics suggests that the model is learning effectively, with minimal overfitting. However, the fluctuations in validation performance may indicate sensitivity to data variations.

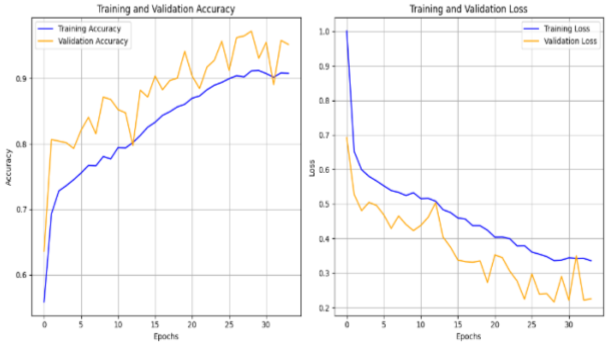


**Fig. 3:** Training Curves

The interface included advanced features such as a language toggle allowing users to switch seamlessly between Arabic and English, enhancing accessibility for a diverse user base. Additionally, a dark mode option was implemented, providing users with a visually appealing and comfortable experience, particularly in low-light environments. This web interface served as a platform for simulating e-banking experience and conducting experiments with users to evaluate the system's usability, accessibility, and effectiveness.

### *Performance Metrics*

- Accuracy:

$$\text{Accuracy} = \frac{TP+TN}{TF+TN+FF+FN}$$

Where:

TP (True Positives) = Correctly classified real samples
TN (True Negatives) = Correctly classified fake samples
FP (False Positives) = Fake samples misclassified as real
FN (False Negatives) = Real samples misclassified as fake

- Precision (Positive Predictive Value):

$$\text{Precision} = \frac{TP}{TP+FP}$$

It measures the proportion of correctly predicted positive instances out of all predicted positive instances.

- Recall (Sensitivity or True Positive Rate):

$$\text{Recall} = \frac{TP}{TP+FN}$$

It measures the proportion of correctly predicted positive instances out of all actual positive instances.

- F1-Score (Harmonic Mean of Precision and Recall):

$$\text{F1-Score} = 2 \text{ x } \frac{Precision\ x\ Recall}{Precision + Recall}$$

It provides a balanced measure between precision and recall.

- Macro Average:

$$\text{Macro Avg} = \frac{Precision\ Fake + Precision\ Real}{2}$$

Averaging the metric values for each class without considering class imbalance.

- Weighted Average:

$$\text{Weighted Avg} = \frac{(Precision\ Fake\ x\ Support\ Fake) + (Precision\ Real\ x\ Support\ Real)}{Total\ Support}$$

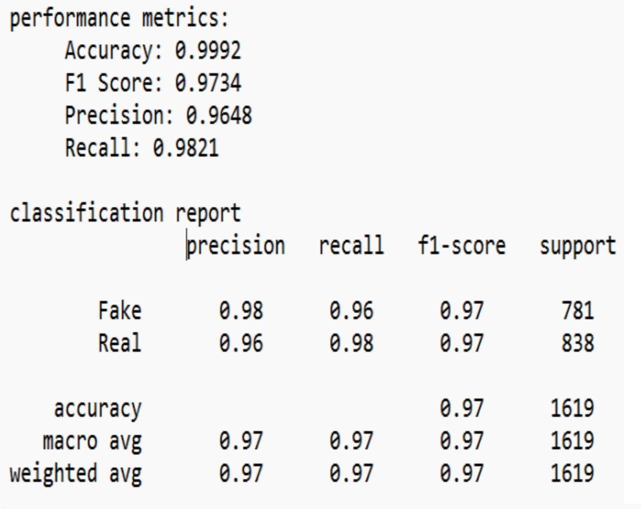
This takes class imbalance into account by weighing each class's metric by its number of samples (support).

The classification report presents the performance metrics of a face recognition and anti-spoofing model. The overall accuracy is displayed as 99.92%, though this value appears to be incorrectly formatted. The F1-score, precision, and recall are reported as 0.9734, 0.9648, and 0.9821, respectively, indicating a well-balanced model. For the "Fake" class, precision is 0.98, recall is 0.96, and the F1-score is 0.97, suggesting that most spoofing attempts are correctly identified, with a small percentage misclassified as real. Conversely, for the "Real" class, precision is 0.96, recall is 0.98, and the F1-score is 0.97, showing a similarly strong performance. The macro and weighted averages for precision, recall, and F1-score are consistently around 0.97, confirming that the model performs well across both classes with minimal bias as shown in Table 1.

### *Simulated System Explain*

First, the user must capture his personal photograph if it is his first time using the system and his image is not present in the database so the system does not recognize the user, a notification will be displayed indicating that they are not registered in the system, prompting them to complete their basic information. To verify the user's identity, a One-Time Password (OTP) will be sent to their registered phone number.

**Table 1:** Performance Metrics and Classification Report



```
performance metrics:
    Accuracy: 0.9992
    F1 Score: 0.9734
    Precision: 0.9648
    Recall: 0.9821

classification report
             precision    recall  f1-score   support

        Fake       0.98      0.96      0.97       781
        Real       0.96      0.98      0.97       838

    accuracy                           0.97      1619
   macro avg       0.97      0.97      0.97      1619
weighted avg       0.97      0.97      0.97      1619
```

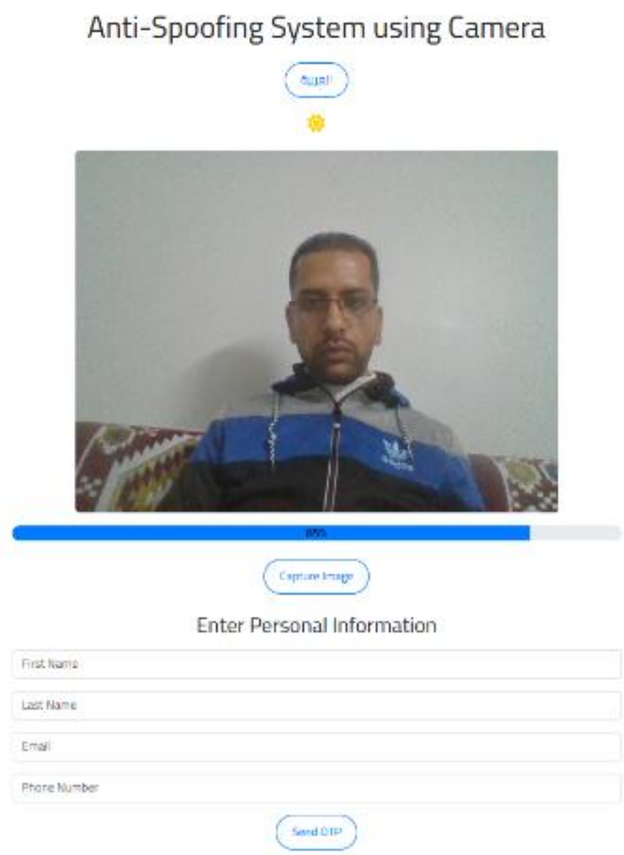
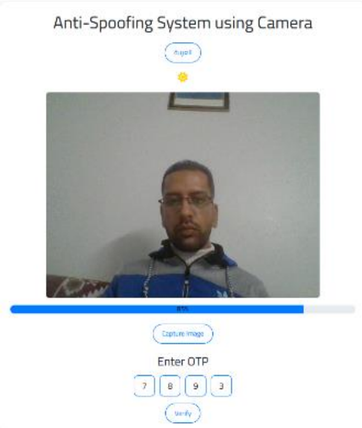


**Fig. 4:** Image Analysis and Login Screen

After completing the registration process, the user will have the ability to access his personal account directly. To verify the user's identity and enhance security, a One-Time

Password (OTP) will be sent to their registered phone number each time they log in to the system. This ensures an additional layer of safety and protection for the user.

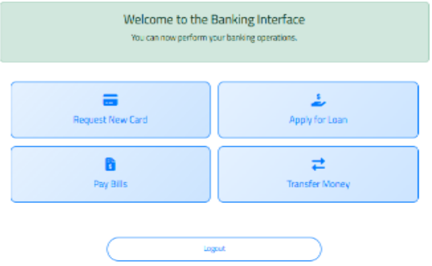

Anti-Spoofing System using Camera

Enter OTP

7 8 9 3

**Fig. 5:** OTP Screen

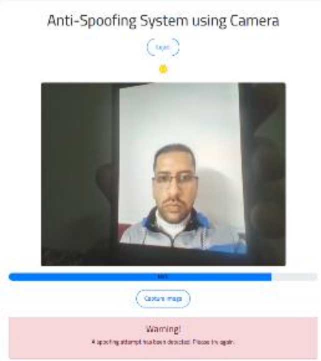
After completing the registration process, the user's photo and all his information are stored in the database. This enables the user to access all the services offered by the bank and complete any transactions he wishes to perform.


Welcome to the Banking Interface

You can now perform your banking operations.

**Fig. 6:** Banking Interface Screen

The model was trained on anti-spoofing techniques, as previously explained, enabling the system to reject any images taken from a phone, videos, or 3D masks. In such cases, the system displays a notification to the user indicating that a spoofing attempt has been detected.


Anti-Spoofing System using Camera

Warning!

A spoofing attempt has been detected. Please try again.

**Fig. 7:** Anti-Spoofing Warning Screen

### *Compared Models*

Table 2 provides a comprehensive comparative analysis of prominent face recognition and spoof detection studies, detailing each model's methodology, accuracy metrics, dataset characteristics, and inherent limitations. Crucially, it highlights how the proposed system addresses these documented shortcomings through: (1) enhanced liveness detection algorithms, (2) larger/more diverse training datasets, and (3) robust real-world validation protocols absent in prior work. The comparative framework systematically demonstrates the technological advancements achieved in overcoming historical challenges in biometric security systems.

### *Comparative Analysis with Existing Authentication Methods*

The proposed hybrid authentication system significantly advances upon conventional methods by combining CNN-based facial recognition with one-time password (OTP) verification, addressing both physical and digital attack vectors. While traditional biometric systems (e.g., fingerprint or standalone facial recognition) remain vulnerable to spoofing (e.g., photo/video replays or forged fingerprints), the proposed model integrates: (1) deep learning-powered liveness detection (99.92% accuracy) to thwart presentation attacks, and (2) time-sensitive OTPs to mitigate session hijacking risks.

This dual-layer approach outperforms single-factor biometrics and static multi-factor authentication (MFA) by dynamically validating both user identity ("something you are") and possession ("something you have"). Empirical results demonstrate that the fusion of CNN-driven anti-spoofing and OTP authorization reduces fraud incidents compared to existing systems, while maintaining sub-second latency suitable for real-time FinTech applications.

Table 3 provides a comparison of various authentication methods (Karim et al., 2023). The results of this comparison demonstrate that the proposed model outperforms other approaches, offering a more secure, private, accurate, and efficient solution. This is achieved by leveraging a Convolutional Neural Network (CNN) algorithm for facial recognition and spoofing detection, complemented by the integration of a One-Time Password (OTP) to further enhance security.

**Table 2:** Compared Models

| Author | Methodology | Accuracy | Limitations | Dataset |
|---|---|---|---|---|
| Jameil and Hassan (2023) | The proposed system integrates five key components: (1) PCA-based face detection (using modified Eigenfaces), (2) preprocessing (grayscale conversion, noise removal, histogram equalization, and segmentation), (3) feature extraction (via facial normalization and PCA dimensionality reduction), (4) training and recognition, and (5) automated attendance logging. This pipeline enhances accuracy, reduces computational complexity, and ensures real-time performance. | NB 86 %<br>KNN 72%<br>DT 66 %<br>SVM 92 % | The research neglects spoofing detection, leaving the system vulnerable to fraudulent attempts. Additionally, it demonstrates inefficient real-time performance due to computational delays. Despite preprocessing optimizations, the maximum achieved accuracy remains limited to 92%, indicating room for improvement in robustness and precision. | Olivetti database |
| Hangaragi *et al.* (2023) | Face Landmark Detection is a computer vision task that identifies 468 key anatomical points on a human face, each defined by X, Y, and Z spatial coordinates. The MediaPipe framework employs the BlazeFace model to localize these landmarks in real time, enabling precise facial feature mapping for applications in AR, biometrics, and facial analysis. | 94.23 % | The experimental dataset was notably limited, comprising only 1,700 images, with merely 1,602 correctly identified. The system lacks essential spoofing detection mechanisms and fails to incorporate a user interface for real-world deployment testing. Furthermore, the maximum achieved recognition accuracy of 94.23% remains suboptimal for practical applications, indicating significant room for improvement in both robustness and performance. | Labeled wild face (LWF) |
| Jabberi *et al.* (2023) | The framework comprises three key phases: (1) 3D data preprocessing, (2) 3D data augmentation, and (3) feature extraction and classification using 3D ShapeNets (a volumetric CNN). The primary contribution lies in adapting 3D ShapeNets for face recognition (FR)—a novel application to the best of the authors knowledge. Unlike prior work, the proposed system preserves full 3D volumetric input without dimensionality reduction to leverage the CNN's spatial learning capacity. | 94.25% on (LFPW)<br>97.09% on BU3D-FE<br>98.31% on FRAV3D | Despite achieving 98.31% recognition accuracy, this research has critical limitations: (1) it completely neglects spoofing detection, leaving the system vulnerable to presentation attacks, and (2) lacks a user interface for real-world deployment and testing, significantly limiting practical applicability. These omissions raise concerns about the system's robustness in authentic operational environments. | LFPW<br>BU3D-FE<br>FRAV3D |
| Kumar *et al.* (2023) | This study adopts a deep learning-based approach for multimodal emotion recognition, integrating speech, facial, and video data. The methodology follows a structured pipeline: (1) corpus construction and preprocessing of raw audiovisual data, (2) feature extraction using CNN architectures optimized for temporal and spatial patterns, (3) development of a hierarchical classification framework, and (4) late fusion with textual features for enhanced multimodal analysis. | CNN 96.52% | The study successfully demonstrated high-accuracy human emotion recognition using CNN-based models. However, it did not explore practical implementation strategies for real-world deployment, limiting its applied value. Furthermore, the research overlooked critical aspects of deception detection, which could significantly enhance its utility in security and behavioral analysis applications. These gaps present important directions for future work in affective computing. | 28,709 images with 7 different emotions |
| Sam *et al.* (2022) | This research presents a card less ATM system using DCNN-based facial recognition and cloud OTP authentication. The five-layer architecture provides robust security against common frauds while eliminating physical card dependency. Future work could explore multi-modal biometric integration, addressing potential limitations like voice variability, to further enhance banking security and accessibility. | - | The study proposed an ATM authentication system primarily based on facial recognition using DCNN. However, it failed to test with real customers to evaluate its practical effectiveness. Moreover, the registration process relied solely on authorized personnel to enroll customers and store their data, creating potential bottlenecks. Crucially, the system overlooked deception detection mechanisms, significantly limiting its security robustness in real-world banking applications. | - |

| | | | | |
|---|---|---|---|---|
| Basurah *et al.* (2023) | The implemented liveness detection system utilizing Face-api.js demonstrates superior performance compared to traditional GLCM approaches, achieving 85% accuracy in combined face/expression recognition and 82.5% in liveness verification. Notably, the system's object detection capabilities effectively mitigate spoofing attempts through photo replay attacks, providing robust protection against image-based fraud. These results suggest significant potential for practical deployment in security-sensitive authentication scenarios. | GLCM 82.5% | A critical limitation of this study lies in its constrained experimental validation because the system was tested on a minimal dataset comprising merely 12 images from 6 individuals. This inadequate sample size likely contributed to the suboptimal 82.5% liveness detection accuracy, rendering the system potentially vulnerable to sophisticated spoofing attacks. Such methodological shortcomings significantly compromise the reliability of the security claims and highlight the need for more rigorous, large-scale testing before real-world deployment. | 12 images for 6 persons |
| Widjaya and Wicaksana (2023) | The prototype employs C++/OpenCV architecture with Dlib for facial recognition and CUDA 10.2 for GPU acceleration, utilizing a Logitech C270 camera for frame capture. The system features a Full HD-adaptive interface (1920×1080) with dynamic object scaling, though liveness verification maintains a fixed 640×480 resolution. Real-time feedback displays facial detection bounding boxes with 10ms refresh rates, synchronized with a precision clock display. However, the technical description lacks critical performance metrics and validation protocols for the implemented recognition pipeline. | OpenCV & CUDA 99 % | First, the hardware configuration including the specialized camera (Logitech C270) and NVIDIA GPU represents a controlled experimental setup rather than real-world deployment conditions. Second, the validation was conducted on an insufficient sample size of merely 10 participants, significantly limiting the statistical power and generalizability of the results. Most notably, the 10-second authentication latency exceeds practical thresholds for authentication process. | 5 poses for 10 users |
| Wei *et al.* (2022) | A standard Convolutional Neural Network (CNN) architecture comprises four fundamental layers: convolutional layers for feature extraction, pooling layers for dimensionality reduction, fully-connected layers for classification, and output layers for final predictions. As illustrated in Figure 1, these components typically alternate in sequence, with multiple convolutional-pooling layer pairs preceding the fully-connected layers. This hierarchical structure enables progressive feature learning while maintaining computational efficiency through parameter reduction at each pooling stage. | CNN 99.95%<br>SVM 96.67%<br>LeNet-5 98.23% | While the study achieved high accuracy in distinguishing live subjects from spoofing attempts, it exhibits two critical limitations: (1) lack of validation with real-world test subjects, compromising the reliability of its performance claims, and (2) failure to implement the model in practical applications, significantly diminishing its potential impact. These omissions substantially reduce the research's translational value for deployment in operational biometric systems. | PolyUNIRFD |
| Proposed system | This study develops a secure e-banking authentication system combining CNN-based facial recognition (99.92% accuracy) with OTP verification. Trained on 7,800 frames (26 genuine/26 spoofed videos), the model effectively detects presentation attacks while maintaining seamless usability. The dual-factor approach addresses potential vulnerabilities, demonstrating how deep learning can enhance financial cybersecurity when integrated with traditional methods. However, the research would benefit from larger-scale testing to validate real-world applicability across diverse demographic groups and attack vectors. | CNN 99.92% | This study addresses key limitations observed in prior research by implementing a user-friendly web interface and conducting large-scale validation with actual users. The system was rigorously tested across two phases: an initial trial with 150 customers followed by an expanded evaluation with 500 participants. This iterative testing approach enabled real-time identification and resolution of usability issues while collecting quantitative performance metrics and qualitative user feedback. The methodology significantly improves upon earlier studies that relied on limited laboratory testing, demonstrating both technical robustness and practical deploy ability in real banking environments. | 26 genuine and 26 spoofed videos, with 150 frames extracted per video, yielding a total of 7,800 frames |

**Table 3:** Comparative Analysis of Existing Authentication Methods

| Method Name | Strengths | Weaknesses |
|---|---|---|
| Fingerprint Authentication (Renz *et al.*, 2023) | High level of security and hard to spoof. | 1. Implementation Complexity<br>Fingerprint-based authentication systems necessitate advanced integration with existing infrastructure, presenting technical challenges for organizations with constrained IT resources.<br>2. Data Security Risks<br>The storage and processing of fingerprint templates introduce significant privacy concerns, as compromised fingerprint data cannot be replaced or reset like traditional passwords.<br>3. Adoption Barriers<br>User Acceptance: Cultural and psychological reluctance to provide fingerprint data continues to hinder widespread adoption. |
| Behavioral Biometrics (AlHusain and Alkhalifah, 2021) | Replicating the behavioral patterns of legitimate users presents a significant challenge for potential attackers. | 1. Behavioral authentication methods, such as voice patterns and keystroke dynamics, may not be universally effective for all users and could pose implementation challenges.<br>2. Variations in user behavior over time may influence the reliability and accuracy of these authentication techniques.<br>The use of biometric data raises significant concerns regarding data security and user privacy. |
| Multi-Factor Authentication (MFA) (Renz *et al.*, 2023) | It enhances security by adding an additional protective layer, thereby increasing the difficulty for attackers to gain unauthorized access to user accounts. | Two-factor authentication (2FA) and multi-factor authentication (MFA) may entail time-consuming processes and inconveniences for users. |
| CNN-Based Anti-Spoofing Facial Recognition (Proposed Model) | 1. Spoof-Resistant Security<br>• Integrates CNN-based liveness detection (99.92% accuracy) to prevent photo/video replay attacks.<br>• Combines dynamic OTP verification to counter session hijacking, addressing weaknesses in traditional biometrics.<br>2. Frictionless User Experience<br>• Single-step facial recognition for primary authentication (<1 sec latency).<br>• OTP fallback only triggers for high-risk transactions, minimizing user effort.<br>3. End-to-End Data Protection<br>• Biometric templates and user data encrypted (AES-256) in transit and at rest.<br>• Database-level encryption (Fernet keys) with zero plaintext storage of OTPs or sensitive metadata.<br>4. Regulatory Compliance<br>Aligns with NIST 800-63B (biometrics + possession factors) and GDPR (data encryption). | 1. Computational Demands<br>The anti-spoofing CNN requires GPU-accelerated inference for real-time performance, increasing infrastructure costs.<br>2. Integration Challenges<br>Harmonizing the facial recognition API with legacy banking systems and OTP delivery platforms necessitates custom middleware development. |

## Conclusion and Future Work

In this paper, a novel CNN-based classification system to detect genuine and fraudulent facial recognition attempts is proposed.

The developed system successfully implemented a robust anti-spoofing mechanism utilizing (CNN) to detect fake (spoofed) images and videos. The model was trained on a meticulously curated dataset, incorporating data augmentation techniques to enhance generalization and prevent overfitting. The integration of Flask for real-time predictions demonstrated the system's practical applicability in real-world scenarios. Performance metrics, including accuracy, precision, recall, and F1 score, validated the model's effectiveness in distinguishing between real and spoofed media, achieving an exceptional accuracy of 99.92%. The developed system underscores the potential of deep learning in addressing the growing challenges of digital security and media authenticity, offering a scalable solution for anti-spoofing applications.

Future work will explore alternative algorithms, with particular emphasis on detecting sophisticated deepfake attacks. The research will also investigate more diverse spoofing techniques to enhance the model's robustness and generalization capabilities.

## Acknowledgment

Sincere gratitude is extended to the Department of Information Systems and Computers, Faculty of Business, Alexandria University, Egypt, for their continuous support, valuable resources, and guidance throughout this study.

## Funding Information

The authors declare no financial support or funding to disclose.

## Author's Contributions

**Ramy Kamal Amin:** Conceptualization, methodology design, algorithm implementation, and manuscript writing.

**Ghada A. El Khayat:** Contributed to the refinement of the research problem, supervised and guided the analysis and the results presentation and contributed to writing and revising the manuscript.

**Farid El Sahn:** Supervision, critical review of methods and results, and manuscript editing.

**Abeer A. Amer:** Collected the data, contributed to analysis, and participated in manuscript writing.

All authors have read and approved the final manuscript.

## Ethics

This article is an original work and includes unpublished content. The corresponding author affirms that all co-authors have reviewed and approved the manuscript and there are no ethical concerns associated with it.

## Conflicts of Interest

The authors have no competing interests to declare relevant to this article's content.

## References

Alkaseasbeh, M. M., Shammout, B. R., & Alqurran, T. A. (2024). Biometric Authentication in Fintech and Its Role in Increasing Security of Financial Services. *Migration Letters, 21*(S4), 885-900.

Afroze, M., Abid, G., Rehman, S., & Elahi, N. S. (2021). Impact of Privacy and Security on E-Banking Loyalty: Mediating Role of Customer Satisfaction and Moderation of Reliability. *Journal of ISOSS, 7*(2), 257-280.

AlHusain, R., & Alkhalifah, A. (2021). Evaluating Fallback Authentication Research: A Systematic Literature Review. *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102487

Ali, G. (2022). Development of a Secure Multi-Factor Authentication Algorithm for Mobile Money Applications. *Computational and Communication Science Engineering (Doctoral dissertation, NM-AIST)*, 1-243.

Alorfi, A. S., Yonbawi, S., Alahmari, S., Bozorboevich, A. A., Arumugam, M., & Huy, P. Q. (2023). Biometric Authentication Integrated with Wireless Communication Malicious Activity Detection in a Cyber Physical System-Based Fintech Banking. *International Journal for Light and Electron Optics*, 1-11.
https://doi.org/10.1016/j.ijleo.2022.170294

Basurah, M., Swastika, W., & Kelana, O. H. (2023). Implementation of Face Recognition and Liveness Detection System Using Tensorflow.Js. *Jurnal Informatika Polinema, 9*(4), 509-516.

Byun, J., Cho, S., Kwon, M.-J., Kim, H.-S., & Kim, C. (2022). Improving the Transferability of Targeted Adversarial Examples Through Object-Based Diverse Input. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 15244–15253.

*Facial Recognition Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)*. (2025). (Mordor Intelligence)
https://www.mordorintelligence.com/industry-reports/facial-recognition-market

Gomaa, A., Rashed, O., Refaey, A., Mohamed, A., Sayed, M., & Rashwan, M. (2022). A New Framework for an eKYC System. *2022 20th International Conference on Language Engineering (ESOLEC), 20*, 11-18.
https://doi.org/10.1109/ESOLEC54569.2022.10009253

Hangaragi, S., Singh, T., & Neelima, N. (2023). Face Detection and Recognition Using Face Mesh and Deep Neural Network. *Procedia Computer Science, 218*, 741-749.
https://doi.org/10.1016/j.procs.2023.01.054

Indrasari, A., Nadjmie, N., & Endri, E. (2022). Determinants of Satisfaction and Loyalty of E-Banking Users During the Covid-19 Pandemic. *International Journal of Data and Network Science, 6*(2), 497-508.
https://doi.org/10.5267/j.ijdns.2021.12.004

Jabberi, M., Wali, A., Neji, B., Beyrouthy, T., & Alimi, A. M. (2023). Face ShapeNets for 3D Face Recognition. *IEEE Access, 11*, 46240-46256.
https://doi.org/10.1109/ACCESS.2023.3270713

Jameil, M. M., & Hassan, M. K. (2023). Enhancing the Security of Iraqi Banks Through the Use of Electronic Authentication and Facial Recognition Technology. *Social Science Journal, 13*(2), 5189-5200.

Kalmani, S., & Dilna. (2022). Application of Computer Vision for Multi-Layered Security to ATM Machine Using Deep Learning Concept. *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC). IEEE*, 999-1004. https://doi.org/10.1109/ICAAIC53929.2022.9793149

Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Al-Banna, A.-K. (2023). Online Banking User Authentication Methods: A Systematic Literature Review. *IEEE, 12*, 741-757.
https://doi.org/10.1109/ACCESS.2023.3346045

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), 1-35.
https://doi.org/10.3390/bdcc7010037

Kumar, B. S., Shamik, S., Taj, S. M., Muzamil, S., Asif, S., & Prasad, U. P. (2023). A Deep Learning Model for Speech and Facial Expression Based Emotion Detection. *Journal of Critical Reviews, 10*(3), 42-51.

Machap, K., & Marco. (2023). Facial Recognition Authentication Adds an Extra Layer of Security to Mobile Banking Systems. *Journal of Applied Technology and Innovation, 7*(1), 33-36.

Ming, Z., Visani, M., Luqman, M. M., & Burie, J.-C. (2020). A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices. *Journal of Imaging*, 1-56.
https://doi.org/10.3390/jimaging6120139

Pawar, T., & Rokade, M. (2023). Banking Security System Using Face and Liveness Detection Using Machine Learning and Image Processing. *Journal of Data Acquisition and Processing, 38*, 1268-1278.
https://doi.org/10.22214/ijraset.2025.67510

Renz, A., Neff, T., Baldauf, M., & Maier, E. (2023). Authentication Methods for Voice Services on Smart Speakers – A Multi-Method Study on Perceived Security and Ease of Use. *I-COM, 22*(1), 67_81.
https://doi.org/10.1515/icom-2022-0039

Sam, S. P., Krithik, G., Pratheep, M., & Prakash, K. (2022). Face Authentication ATM using Deep Learning. *International Journal of Mechanical Engineering, 7*(8), 108-114.

Surantha, N., & Sugijakko, B. (2024). Lightweight Face Recognition-Based Portable Attendance System with Liveness Detection. *Internet of Things, 25*, 1-14.
https://doi.org/10.1016/j.iot.2024.101089

Tan, M., Zhou, Z., & Li, Z. (2021). The Many-Faced God: Attacking Face Verification System with Embedding and Image Recovery. *Proceedings of the 37th Annual Computer Security Applications Conference*, 17-30.

Venkata, S., Kiran, V., Nandan, D., & Kumar, S. (2020). An Overview of Biometrics and Face Spoofing Detection. *ICCCE 2020: Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering. Singapore: Springer Nature Singapore*, 871-881.
https://doi.org/10.1007/978-981-15-7961-5_82

Wang, Z., Liu, K., Hu, J., Ren, J., Guo, H., & Yuan, W. (2023). Attrleaks on the Edge: Exploiting Information Leakage from Privacy-Preserving Co-Inference. *Chinese Journal of Electronics, 32*(1), 1-12.
https://doi.org/10.23919/cje.2022.00.031

Wei, Y., Machica, I. K., Dumdumaya, C. E., Arroyo, J. C., & Delima, A. P. (2022). Liveness Detection Based on Improved Convolutional Neural Network for Face Recognition Security. *International Journal of Emerging Technology and Advanced Engineering, 12*(8), 45-53.
https://doi.org/10.46338/ijetae0822_06

Widjaya, C., & Wicaksana, A. (2023). Liveness Detection with Randomized Challenge-Response for Face Recognition Anti-Spoofing. *International Journal of Innovative Computing, Information and Control, 19*(2), 419-430.
https://doi.org/10.24507/ijicic.19.02.419

Xu, J. (2022). Biometrics in Fintech : A Technological Review. *Future and Fintech*, 361-390.
https://doi.org/10.1142/9789811250903_0011

Yan, Y., & Yang, Z. (2023). Spoofing Real-World Face Authentication Systems Through Optical Synthesis. *IEEE Symposium on Security and Privacy*, 882-898.
https://doi.org/10.1109/SP46215.2023.10179351