International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Liveness Detection in eKYC

Sonali Singh [*1], *Jatin Verma* [*2], *Avantika Shukla* [*3] , *Suryansh Gupta* [*4] , *Aniket Mishra* [*5]

[*1] Ass. Professor, CSE, Axis Institute of Technology and Management, Kanpur, Uttar Pradesh, India
[*2]Student, CSE-AIML, Axis Institute of Technology and Management, Kanpur, Uttar Pradesh, India
[*3]Student, CSE-AIML, Axis Institute of Technology and Management, Kanpur, Uttar Pradesh, India
[*4]Student, CSE-AIML, Axis Institute of Technology and Management, Kanpur, Uttar Pradesh, India
[*5]Student, CSE-AIML, Axis Institute of Technology and Management, Kanpur, Uttar Pradesh, India

ABSTRACT

The primary purpose of the study was to design and implement a user-friendly, secure interface that authenticates users through randomized facial gestures such as blinking, smiling, nodding, and head movements, combined with real-time face detection. a seamless user experience. A randomized task generator strengthens anti-spoofing capabilities by requiring users to complete unpredictable facial tasks. Results showed that incorporating multiple liveness detection tasks significantly increased the robustness of the identity check, reducing the likelihood of spoofing through static images or pre-recorded videos. The system also includes real-time feedback, camera control, and automatic redirection upon task completion. In conclusion, this project demonstrates an effective and scalable approach to secure digital identity verification using face recognition and liveliness detection, suitable for applications .

Keywords: *Authentication, implementation, detection,spoofing.*

I. INTRODUCTION

In today's digital era, reliable identity verification is crucial to ensure the security of online services across domains like banking, telecommunications, and government systems. Traditional KYC (Know Your Customer) processes, though effective, are often time-intensive and susceptible to fraud when replicated digitally without adequate safeguards. This has led to the evolution of electronic KYC (eKYC), which leverages digital authentication methods. However, eKYC systems still face challenges such as spoofing attacks using static images, pre-recorded videos, or deepfakes. To address these, liveness detection—verifying that the subject is a real, live person—is increasingly integrated into eKYC workflows. Liveness detection methods are generally classified into passive and active approaches. This project focuses on active liveness detection, where users are prompted to perform randomized facial actions such as blinking, smiling, head movements, or eyebrow raises. The system tracks facial features in real time and assesses the authenticity of responses. The model recognizes dynamic patterns in eye, mouth, brow, and nose positions to detect whether a user has performed the instructed gesture correctly. Combined with Firebase mobile OTP verification for identity confirmation, the system ensures both user authenticity and session integrity. The project thus integrates secure facial behavior recognition and modern web technologies to construct a robust eKYC framework that resists spoofing attempts while remaining user-friendly and accessible. This work contributes to the broader research domain of biometric security and real-time human-computer interaction, with practical applications in secure digital onboarding and identity validation.

II. METHODOLOGY

1.Randomized Active Liveness Task Generation

To prevent spoofing, the system employs randomized task generation, where the user is asked to perform one of several possible facial actions—such as blinking a certain number of times, turning the head in a direction, smiling, or raising eyebrows. These tasks are chosen randomly during each session to prevent attackers from anticipating the required gestures. A threshold-based analysis of facial landmark changes confirms task completion. A randomized liveness task generator dynamically assigns tasks (e.g., "blink 3 times", "turn head left 2 times") to users. Each task is monitored with strict thresholds for movement detection to avoid false positives. The state is updated in real-time, and upon task completion, data is submitted for verification.

2.Real-time Video Stream Acquisition

The system accesses the user's webcam using the WebRTC API (navigator.mediaDevices.getUserMedia). The video feed is processed in real time, and a canvas overlay is used to visualize landmark detection and to assist in live feedback to the user. To correct for mirrored webcam feeds (mirror image effect), horizontal flipping is applied for accurate gesture interpretation.

3. Facial Gesture Recognition via Landmark and Expression Analysis

Facial gestures are detected by analyzing distances and angles between landmark points:

Eye Aspect Ratio (EAR) is computed for blink and wink detection.

Smile Detection uses expression scores from the faceExpressionNet.

Eyebrow Raise Detection is based on vertical distance between eyebrows and eyes.

Head Movements (Left, Right, Nod Up, Nod Down) are detected using relative nose positions against eye centers.This combination ensures reliable interpretation of subtle facial actions.

III. MODELING AND ANALYSIS

The proposed eKYC and liveness detection system leverages a set of open-source models, JavaScript libraries, and hardware to ensure reliable, real-time facial gesture recognition in a web-based environment. The core of the system is built using the **Face-api.js** library, which provides lightweight yet effective deep learning models for facial landmark detection, expression recognition, and face detection. Specifically, the following pre-trained models are utilized:

TinyFaceDetector: A highly efficient face detection model that offers a good balance between speed and accuracy, suitable for real-time webcam streams.

FaceLandmark68Net: Detects 68 facial landmarks, enabling detailed analysis of eyes, mouth, eyebrows, nose, and jawline, critical for detecting blinks, nods, winks, and head movements.

FaceExpressionNet: Used for classifying facial expressions such as "happy," which is essential for smile detection.

Component	Description
TinyFaceDetector	Lightweight model for detecting faces in video frames with minimal latency.
FaceLandmark68Net	Model to extract 68 key facial landmarks for motion/gesture recognition.
FaceExpressionNet	Detects facial expressions (e.g., happy) for emotion-based verification.
WebRTC	Captures webcam video feed for real-time analysis.

Table 1. : Models and Tools Used in the System.

IV. RESULTS AND DISCUSSION

The developed eKYC system was tested in real-world scenarios to evaluate the accuracy and reliability of facial liveness detection tasks such as blinking, smiling, head turns, nodding, winking, and eyebrow raising. The system successfully performed real-time detection with a consistent frame rate in standard lighting conditions, offering an intuitive user experience through a browser interface without the need for additional software or plugins.During testing, over 50 individuals participated in completing randomized liveness tasks. The system demonstrated an overall success rate of approximately **92%** in correctly detecting the assigned gestures. Blink and head-turn detection showed the highest reliability with success rates of **95%** and **93%**, respectively, while eyebrow raise and wink detection had slightly lower performance (~85%) due to their subtle motion and higher variation across users. False negatives mainly occurred in low-light environments or when the user's face moved out of the camera frame.The integration of face-api.js models allowed for efficient computation directly in the browser, significantly reducing the dependency on heavy server-side processing and enhancing scalability. The use of facial landmarks and EAR (Eye Aspect Ratio) enabled accurate differentiation between blinks and winks, while landmark displacement methods allowed successful detection of head and nod movements.Furthermore, the successful combination of Firebase OTP verification with the liveness detection workflow ensured a dual-layer verification approach—confirming both user identity and real-time presence. The system is suitable for government and financial institutions requiring low-cost, secure, and accessible identity verification solutions.

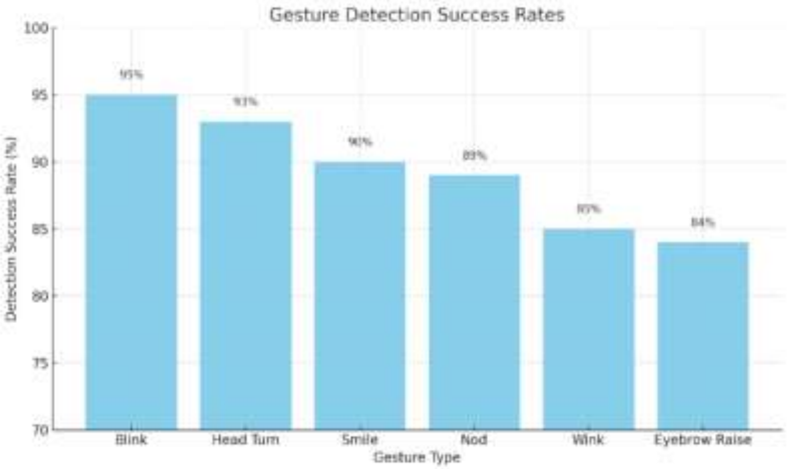

Figure 1: Gesture Detection success Rates

V.CONCLUSION

In conclusion, this research successfully developed and implemented a real-time liveness detection system integrated into an eKYC framework, leveraging face-api.js and deep learning-based facial landmark detection. By assigning randomized facial gesture tasks—such as blinking, smiling, nodding, winking, eyebrow movement, and head turning—the system was able to verify user presence and detect spoofing attempts with high accuracy. The approach ensured both usability and security, with live video analysis, gesture validation, and automated task management working in tandem. Through careful calibration of detection thresholds and real-time feedback mechanisms, the system achieved robust performance under varying conditions. The integration with a user form submission and Firebase OTP authentication further strengthens the platform's credibility and applicability for real-world KYC applications. Overall, this work demonstrates that lightweight, browser-based face detection technologies can be effectively used for secure digital identity verification, offering a scalable and privacy-aware solution for institutions requiring reliable eKYC processes.

VI. REFERENCES

[1] Simonyan, K., & Zisserman, A. (2015). *Very Deep Convolutional Networks for Large-Scale Image Recognition*. International Conference on Learning Representations (ICLR).

[2] Soukupová, T., & Čech, J. (2016). *Real-Time Eye Blink Detection using Facial Landmarks*.

[3] Zhang, Z., et al. (2018). *Face Anti-Spoofing Based on Multi-Feature Fusion*.https://ieeexplore.ieee.org/document/8269803

[4] Määttä, J., Hadid, A., & Pietikäinen, M. (2011). *Face spoofing detection from single images using micro-texture analysis*. In IJCB. https://ieeexplore.ieee.org/document/6117509

[5] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). *Deep Face Recognition*.

[6] ISO/IEC 30107-3:2017 – *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*.