Digital Customer Acquisition With a Viability Control Process

Sabancı Üniversitesi FACULTY OF ENGINEERING AND NATURAL SCIENCES

Student(s)
Arif Kemal Sarı
Bengi Ada Tüfekci

Faculty Member(s)
Erchan Aptoula

Company Advisor(s)
Sabri Can Çetindağ
Saniye Demir

ABSTRACT

Digital onboarding in finance and government increasingly relies on face recognition. Most systems utilize active liveness checks, and they remain manual (rule-based), offering limited automation and insufficient protection against advanced spoofing attempts such as high-resolution printouts and realistic 3D masks. Mobile and embedded platforms further constrain computational resources, making heavyweight models unsuitable. A lightweight, real-time solution tailored to these environments is essential to improve security, reduce fraud, and enable efficient customer acquisition.

This project focused on developing a robust and lightweight facial liveness detection system to support secure digital customer onboarding, particularly on mobile and embedded platforms. The primary objective was to detect common spoofing attacks, such as printed photos, replayed videos, and 3D masks, while operating under strict computational constraints. We propose an ensemble-based approach using MobileNetV2 for facial liveness detection, aimed at improving robustness across different illumination conditions and environments by using a model for each spoof type.

OBJECTIVES

- Develop a robust and lightweight computer vision model to detect various face spoof attacks.

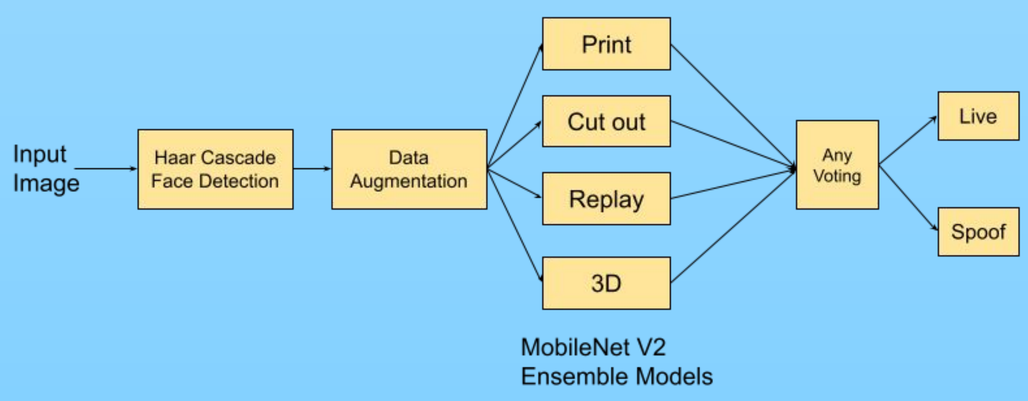
PROJECT DETAILS

The project began with exploring various approaches, including texture-based models using Local Binary Patterns (LBP), traditional classifiers, and baseline CNN architectures. We experimented with multiple input formats (grayscale, RGB, LBP), feature extraction methods, and model configurations. Performance across these variations was benchmarked on two public datasets: CelebASpoof [1] and LCCFASD[2]. We trained our models on CelebASpoof and tested on LCCFASD to assess domain generalizability.

As the project progressed, we shifted toward transfer learning, using MobileNetV2 as the backbone for its balance of speed and efficiency. Various data augmentation strategies—including AutoAugment, RandAugment, Mix Style, and AugMix—were evaluated to improve model robustness. To handle generalization across spoof types, we adopted an ensemble strategy—training four specialized MobileNetV2 classifiers, each focused on a specific attack category. The ensemble outputs were merged using an “any-voting” mechanism, improving robustness across spoof categories.

In parallel, we also investigated a Fourier Transform-based auxiliary loss within a MobileNetV3 variant to capture frequency-domain spoof artifacts; while promising, this approach was not integrated into the final deployed model because of lower performance. The final ensemble achieves 94% accuracy (HTER: 0.05) on CelebASpoof and 78% accuracy (HTER: 0.25) on LCCFASD.

WORKFLOW



METHOD

Local Binary Patterns (LBP): LBP histograms with varying radii were used to capture fine-grained texture differences between real and spoofed faces.
Transfer Learning Using MobileNetV2: A pre-trained MobileNetV2 was further fine-tuned using our datasets.
Data Augmentation: Both standard (e.g., flips, rotations) and advanced augmentations (e.g., AutoAugment, MixStyle) were applied to improve generalization.
Fourier Transform Loss Variant: A MobileNetV3 variant included an auxiliary Fourier loss to enhance sensitivity to spoofing artifacts in the frequency domain.
Evaluation Metrics:
Accuracy measures the overall proportion of correct predictions (both live and spoof).
Macro F1 Score reflects the harmonic mean of precision and recall, averaged across live and spoof classes, ensuring balanced performance.
Half Total Error Rate (HTER) provides a balanced summary of both FAR (False Acceptance Rate) and FRR (False Rejection Rate), commonly used for liveness detection tasks.

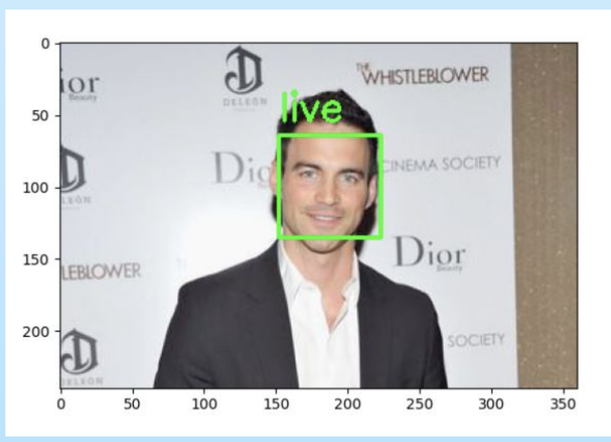


Fig 1. A live face detected as live

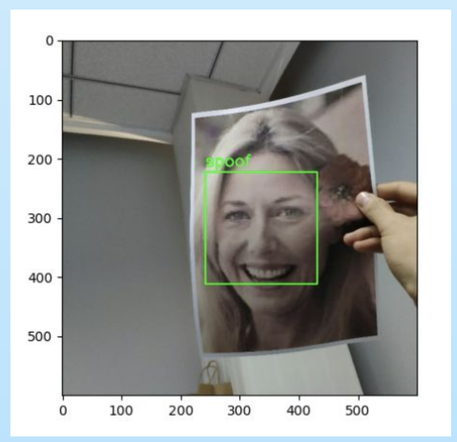


Fig 2. A print attack detected as spoof

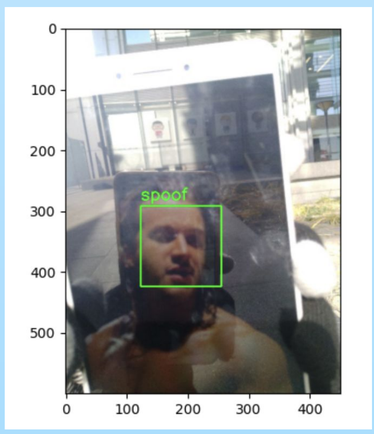


Fig 3. A replay attack detected as spoof

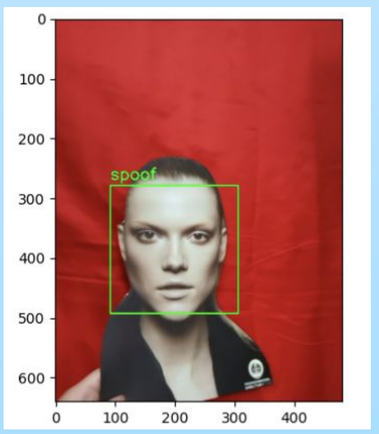


Fig 4. A print cut attack detected as spoof

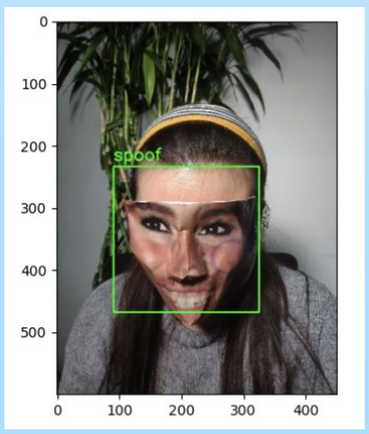


Fig 5. A 3D mask attack detected as spoof

QUANTITATIVE RESULTS

The ensemble model (which was trained on CelebASpoof) was evaluated on the test set of CelebASpoof and LCCFASD public datasets:

	Accuracy	Macro F1 Score	FAR	FRR	HTER
CelebASpoof	0.94	0.93	0.0217	0.803	0.0510
LCCFASD	0.78	0.55	0.2771	0.2146	0.2458

CONCLUSION

While domain generalization remains a challenge, we developed a lightweight and robust computer vision model for liveness detection, capable of detecting various spoof attacks such as print, print cut, replay, and 3d mask attacks under various lighting and environment conditions.

REFERENCES

[1] Y. Zhang et al., CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations. 2020. [Online]. Available: https://arxiv.org/abs/2007.12342

[2] D. Timoshenko, K. Simonchik, V. Shutov, P. Zhelezneva and V. Grishkin, "Large Crowdcollected Facial Anti-Spoofing Dataset," *2019 Computer Science and Information Technologies (CSIT)*, Yerevan, Armenia, 2019, pp. 123-126, doi: 10.1109/CSITechnol.2019.8895208.