



Face Passive Liveness: Presentation-Attack Detection on CelebA-Spoof

Measured 28 October 2026 · iApp Technology Co., Ltd., Bangkok, Thailand

Executive summary. The iApp Passive Liveness API decides from one image whether a face belongs to a live person or is a presentation attack. Through the public API we sent it a seeded sample of the official test split of CelebA-Spoof, a large public face anti-spoofing benchmark: 300 attack images, 30 of each of ten attack types from printed photographs and paper masks to screens and 3D masks, and 200 of the dataset's live images. The API accepted none of the 300 attacks (APCER 0.0%; 95% upper bound 1.0%). It rejected 79.5% of the dataset's live images, which are web photographs of celebrities rather than camera captures; of 69 public selfies taken with phones, it rejected 3 (4.3%, 95% CI [0.0, 10.1]). The decision is strict: it suits images captured live by a camera, not photographs uploaded from a gallery or taken from the web.

1 Introduction

A passive liveness check decides, from a single image and without asking the user to move, whether the face in front of the camera belongs to a live person or is a presentation attack: a printed photograph, a picture on a screen, a paper mask or a three-dimensional mask. It is the step of an identity check that stops a stolen photograph from passing a face match. The iApp API returns a verdict, REAL or SPOOF, with a score.

Two errors matter, and this paper reports both with the error rates defined in ISO/IEC 30107-3: the attack presentation classification error rate (APCER), the share of attacks accepted as live, and the bona fide presentation classification error rate (BPCER), the share of live faces rejected. This is a benchmark measurement on public data, not a conformance test.

2 Test Data

CelebA-Spoof [1] was, at its publication, the largest public face anti-spoofing dataset: 625,537 images of 10,177 people, each annotated with one of ten attack types, the illumination and the capture environment. Its official intra-dataset test split holds 67,170 images of people who are not in its training split. From that split we drew, with seed 1337, 200 live images and 30 images of each of the ten attack types (300 attacks), and sent each image as distributed, full frame.

The live images of CelebA-Spoof are photographs of celebrities collected from the web, not selfies taken for an identity check; the attacks were recorded with consumer phones and tablets in varied settings. Because a liveness check for identity verification is meant to receive camera captures, we also sent 69 genuine phone selfies from three small public samples published for anti-spoofing work (29, 10 and 30 images; Creative Commons BY-NC, BY-ND and BY-NC-ND licences). CelebA-Spoof is licensed for non-commercial research use only. No image is reproduced in this paper.

3 Method

Every image was sent, two requests at a time and with no parameters, to the public endpoint

POST <https://api.iapp.co.th/v3/store/ekyc/face-passive-liveness>

The API's verdict (predict) was taken as its decision. An image is an accepted attack when an attack image is returned as REAL, and a rejected live face when a live image is returned as SPOOF. Requests that returned an error are counted separately. APCER is reported for each attack type and pooled over the ten types (each type has equal weight by design of the sample); the average classification error rate (ACER) is the mean of the pooled APCER and the BPCER. We also report the area under the ROC curve of the returned SPOOF score. 95% confidence intervals are percentile bootstrap intervals (2,000 resamples, seed 1337), resampling live and attack images separately for ACER.

4 Results

Table 1: Errors at the API's own decision. When no attack is accepted, the 95% upper bound is $3/n$. An image declined without a verdict counts as not accepted.

Measure	Images	Value (%) [95% CI]
APCER: attacks accepted, pooled	300	0.0 (upper bound 1.0)
BPCER: phone selfies rejected	69	4.3 [0.0, 10.1]
BPCER: CelebA-Spoof live images rejected	200	79.5 [74.0, 85.0]
ACER, CelebA-Spoof	500	39.8 [36.8, 42.2]
ROC AUC of the SPOOF score, CelebA-Spoof	500	0.979
Declined without a verdict (image too dark)	500	18 images

Table 2: APCER by attack type (30 images each).

Attack type	Group	Accepted as live	APCER (%) [95% CI]
Photo	Print	0 of 30	0.0 (upper bound 10.0)
Poster	Print	0 of 30	0.0 (upper bound 10.0)
A4 print	Print	0 of 30	0.0 (upper bound 10.0)
Face mask (paper)	Paper cut	0 of 30	0.0 (upper bound 10.0)
Upper-body mask (paper)	Paper cut	0 of 30	0.0 (upper bound 10.0)
Region mask (paper)	Paper cut	0 of 30	0.0 (upper bound 10.0)
Computer screen	Replay	0 of 30	0.0 (upper bound 10.0)
Tablet screen	Replay	0 of 30	0.0 (upper bound 10.0)
Phone screen	Replay	0 of 30	0.0 (upper bound 10.0)
3D mask	3D mask	0 of 30	0.0 (upper bound 10.0)

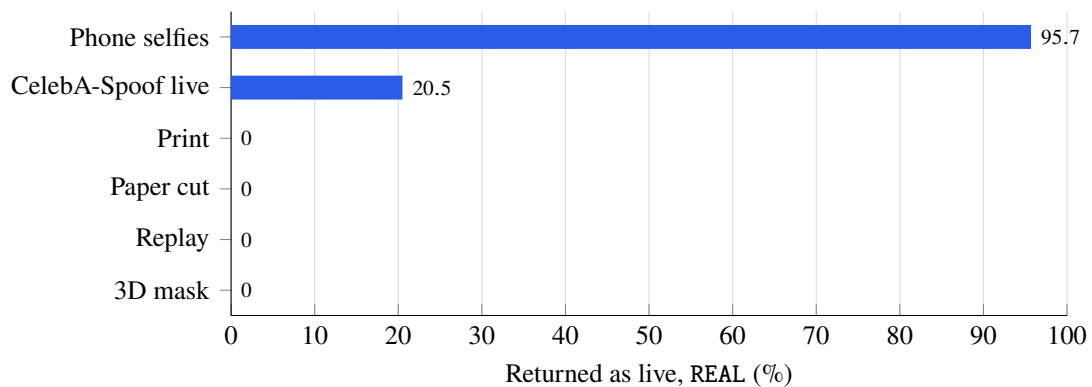


Figure 1: Share of images returned as live: genuine phone selfies, CelebA-Spoof live images, and the four attack groups (print, paper cut, replay, 3D mask).

5 Discussion

No attack was accepted. Across all ten attack types, including screen replays and 3D masks, every attack image was returned as SPOOF or declined; the highest REAL score given to any attack was 5.0×10^{-5} . With 30 images per type, this bounds each type's APCER below 10.0% at 95% confidence, and the pooled APCER below 1.0%.

The live class of CelebA-Spoof is rejected; real selfies are not. The API rejected 79.5% of CelebA-Spoof's live images, which gives that benchmark's ACER of 39.8%. These images are web photographs, often edited and recompressed, and for a liveness check they are not live captures. On 69 genuine phone selfies the rejection rate was 4.3%. The scores separate the CelebA-Spoof classes well (ROC AUC 0.979), but the live images sit far below the decision boundary: a caller that accepted any REAL score of 10^{-4} or more would admit 53.0% of them and still 0.0% of the attacks. We do not recommend lowering the boundary for identity checks; the numbers show how far the default favours security.

Dark images are declined. 18 images (5 live, 13 attacks) were returned without a verdict, with the message THIS_IMAGE_IS_DARK. A caller should ask the user to retake the photograph in better light.

The claim the evidence supports: on the public CelebA-Spoof benchmark, the API accepted none of 300 attacks of ten types, and it rejected 4.3% of 69 genuine phone selfies. Its decision suits camera captures; photographs taken from the web are likely to be rejected.

6 Production Performance

Measured from a client in Bangkok, with two requests in flight, the median end-to-end time through the public API was 0.34 s (90th percentile 0.45 s), including the upload of full-frame images of up to 10.1 MB. The service reported a median processing time of 0.21 s. A check costs 0.3 IC.

7 Limitations

- **Sample size.** 30 images per attack type and 69 selfies give wide intervals; a larger bona fide selfie set, captured on the phones of the intended users, is needed for a precise BPCER.
- **Live images.** The CelebA-Spoof live images are web photographs, not phone selfies, and the 69 selfies come from small public samples of mixed origin; neither represents Thai users specifically.
- **One dataset.** Attack instruments and capture devices differ between datasets; results on one dataset do not transfer exactly to another, or to attacks not represented in it.
- **Licence.** CelebA-Spoof is available for non-commercial research use only.

8 Reproducibility

The scripts `get_data.py`, `bench.py` and `gen_results.py`, the image list with its seed, and the returned verdicts and scores are available from iApp Technology on request: sale@iapp.co.th. The images themselves must be obtained from the dataset's authors.

References

- [1] Y. Zhang, Z. Yin, Y. Li, G. Yin, J. Yan, J. Shao, Z. Liu. *CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations*. European Conference on Computer Vision (ECCV), 2020.

About iApp Technology. iApp Technology Co., Ltd. is a Thai artificial-intelligence company providing OCR, document understanding, speech, identity verification and large-language-model services for the Thai language.
Web: iapp.co.th · E-mail: sale@iapp.co.th · Tel: +66 2 124 4041