

NIST Internal Report NIST IR 8491

Face Analysis Technology Evaluation (FATE)

*Part 10: Performance of Passive, Software-Based Presentation
Attack Detection (PAD) Algorithms*

Mei Ngan
Patrick Grother
Austin Hom

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8491>

NIST Internal Report
NIST IR 8491

Face Analysis Technology Evaluation
(FATE)

Part 10: Performance of Passive, Software-Based Presentation
Attack Detection (PAD) Algorithms

Mei Ngan
Patrick Grother
Austin Hom
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8491>

September 2023



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST Technical Series Policies

[Copyright, Fair Use, and Licensing Statements](#)

[NIST Technical Series Publication Identifier Syntax](#)

Publication History

Approved by the NIST Editorial Review Board on 2023-09-19

How to cite this NIST Technical Series Publication:

Mei Ngan, Patrick Grother, Austin Hom (2023) Face Analysis Technology Evaluation (FATE) Part 10: Performance of Passive, Software-Based Presentation Attack Detection (PAD) Algorithms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8491.
<https://doi.org/10.6028/NIST.IR.8491>

Contact Information

frvt@nist.gov

Abstract

This report quantifies the accuracy of passive face presentation attack detection (PAD) algorithms (software only, no hardware solutions) operating on conventional 2D imagery of various presentation attack instruments (PAI). The algorithms were submitted to the Presentation Attack Detection track of the Face Analysis Technology Evaluation (FATE) executed by the National Institute of Standards and Technology (NIST).

Acknowledgements

The authors would like to thank the Department of Homeland Security's Science and Technology Directorate Biometric and Identity Technology Center, Intelligence Advanced Research Projects Activity, and Johns Hopkins University Applied Physics Laboratory for their contributions to this activity.

The authors are also grateful to the staff in the NIST Biometrics Research Laboratory for infrastructure supporting rapid evaluation of algorithms.

And last but not the least, the authors would like to thank Jack Allen and Jim Matey for their time and candor in reviewing the contents of this report and for providing many meaningful suggestions to help make this a better publication.

Other Relevant Reports

Results from the Face Recognition Technology Evaluation (FRTE) and Face Analysis Technology Evaluation (FATE) activities appear in the series of NIST Interagency Reports tabulated below. From 1999 to July 2023, FRTE and FATE were collectively known as FRVT.

Date	Link	Title	NISTIR
2014-03-20	PDF	FATE Performance of Automated Age Estimation Algorithms	7995
2015-04-20	PDF	FATE Performance of Automated Gender Classification Algorithms	8052
2014-05-21	PDF	FRTE Performance of Face Identification Algorithms	8009
2017-03-07	PDF	Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects	8173
2017-11-23	PDF	The 2017 IARPA Face Recognition Prize Challenge (FRPC)	8197
2020-01-03	Draft	FRTE - Part 1: Verification	Draft
2019-09-11	PDF	FRTE - Part 2: Identification	8271
2019-12-11	PDF	FRTE - Part 3: Demographic Effects	8280
2020-03-04	PDF	FATE - Part 4: MORPH - Performance of Automated Face Morph Detection	8292
2020-03-06	Draft	FATE - Part 5: Face Image Quality Assessment	Draft
2020-07-24	PDF	FRTE - Part 6A: Face Recognition Accuracy with Face Masks using Pre-COVID-19 Algorithms	8311
2022-01-20	PDF	FRTE - Part 6B: Face Recognition Accuracy with Face Masks using Post-COVID-19 Algorithms	8331
2022-07-13	PDF	FRTE - Part 7: Identification for Paperless Travel and Immigration	8381
2022-09-30	PDF	FRTE - Part 8: Summarizing Demographic Differentials	8429
2022-09-30	PDF	FRTE - Part 9A: Face Recognition Verification Accuracy on Distinguishing Twins	8439
2023-09-20	PDF	FATE - Part 10: Performance of Passive, Software-based Presentation Attack Detection (PAD) Algorithms	8491
2023-09-20	PDF	FATE - Part 11: Face Image Quality Vector Assessment: Specific Image Defect Detection	8485

Details appear on pages linked from <https://www.nist.gov/programs-projects/face-projects>.

Key words

Face Analysis Technology Evaluation; FATE; PAD; presentation attack detection.

Table of Contents

Executive Summary	1
Technical Summary	2
1. Presentation Attack Detection (PAD)	7
1.1. Introduction	7
1.2. Scope	7
1.2.1. Physical (Analog) vs. Digital Attacks	7
1.2.2. Passive PAD Approaches vs. User Interaction Required PAD	8
1.2.3. Software vs. Hardware-based PAD	8
1.2.4. Offline Testing	9
2. Datasets	9
2.1. Description of Disclosed PAIs	11
2.2. Description of Imagery	11
3. Metrics	12
3.1. Attack Presentation Classification Error Rate (APCER)	12
3.2. Bona Fide Presentation Classification Error Rate (BPCER)	12
3.3. Failure to Process Events	12
3.4. Detection Error Tradeoff (DET)	13
4. Participation	14
5. Results	17
5.1. Impersonation	17
5.2. Evasion	19
5.3. Stills vs. Videos	23
5.3.1. Impersonation	23
5.3.2. Evasion	28
5.4. Fusion	32
5.4.1. Impersonation	32
5.4.2. Evasion	32
5.5. Demographic Effects	33
References	36
Appendix A. Detailed Algorithm Results	37

A.1. Timing	37
A.2. Impersonation	40
A.3. Evasion	88
Appendix B. Stills vs. Videos	109
B.1. Impersonation	109
B.2. Evasion	123
Appendix C. Demographic Effects	128
C.1. Impersonation	128
C.2. Evasion	138
Appendix D. Abbreviations	142

List of Tables

Table 1. Top Performers - Use Case: detectImpersonationPA - Media Type: stills .	4
Table 2. Top Performers - Use Case: detectEvasionPA - Media Type: stills	4
Table 3. Software vs. hardware-based PAD	9
Table 4. Dataset - Bona Fides	10
Table 5. Dataset - Use Case: detectImpersonationPA	10
Table 6. Dataset - Use Case: detectEvasionPA	10
Table 7. Participant Information	15
Table 8. Results: PA Type 1, detectImpersonationPA, stills	17
Table 9. Results: PA Type 3, detectImpersonationPA, stills	17
Table 10. Results: PA Type 4, detectImpersonationPA, stills	18
Table 11. Results: PA Type 7, detectImpersonationPA, stills	18
Table 12. Results: PA Type 8, detectImpersonationPA, stills	18
Table 13. Results: PA Type 8 (zoomed), detectImpersonationPA, stills	19
Table 14. Results: PA Type 1, detectEvasionPA, stills	19
Table 15. Results: PA Type 2, detectEvasionPA, stills	20
Table 16. Results: PA Type 3, detectEvasionPA, stills	20
Table 17. Results: PA Type 4, detectEvasionPA, stills	20
Table 18. Results: PA Type 5, detectEvasionPA, stills	21
Table 19. Results: PA Type 6, detectEvasionPA, stills	21
Table 20. Results: PA Type 7, detectEvasionPA, stills	22
Table 21. Results: PA Type 8, detectEvasionPA, stills	22
Table 22. Results: PA Type 8 (zoomed), detectEvasionPA, stills	22
Table 23. Results: PA Type 9, detectEvasionPA, stills	23
Table 24. Results: detectImpersonationPA, Stills vs. Videos	23
Table 25. Results: detectEvasionPA, Stills vs. Videos	28
Table 26. Fusion Results: detectImpersonationPA, stills	32
Table 27. Fusion Results: detectEvasionPA, stills	32
Table 28. Demographic Data Summary, Bona Fide Stills	33

Table 29. Timing Statistics	37
Table 30. Appendix: PA Type 1, detectImpersonationPA, stills	40
Table 31. Appendix: PA Type 3, detectImpersonationPA, stills	43
Table 32. Appendix: PA Type 4, detectImpersonationPA, stills	45
Table 33. Appendix: PA Type 7, detectImpersonationPA, stills	47
Table 34. Appendix: PA Type 8, detectImpersonationPA, stills	49
Table 35. Appendix: PA Type 8 (zoomed), detectImpersonationPA, stills	51
Table 36. Appendix: PA Type 1, detectImpersonationPA, videos	54
Table 37. Appendix: PA Type 3, detectImpersonationPA, videos	56
Table 38. Appendix: PA Type 8, detectImpersonationPA, videos	58
Table 39. Appendix: PA Type 1, detectEvasionPA, stills	88
Table 40. Appendix: PA Type 2, detectEvasionPA, stills	89
Table 41. Appendix: PA Type 3, detectEvasionPA, stills	90
Table 42. Appendix: PA Type 4, detectEvasionPA, stills	91
Table 43. Appendix: PA Type 5, detectEvasionPA, stills	92
Table 44. Appendix: PA Type 6, detectEvasionPA, stills	93
Table 45. Appendix: PA Type 7, detectEvasionPA, stills	94
Table 46. Appendix: PA Type 8, detectEvasionPA, stills	95
Table 47. Appendix: PA Type 8 (zoomed), detectEvasionPA, stills	96
Table 48. Appendix: PA Type 9, detectEvasionPA, stills	97
Table 49. Appendix: PA Type 1, detectEvasionPA, videos	98
Table 50. Appendix: PA Type 3, detectEvasionPA, videos	99
Table 51. Appendix: PA Type 5, detectEvasionPA, videos	100
Table 52. Appendix: PA Type 8, detectEvasionPA, videos	101
Table 53. Appendix: PA Type 9, detectEvasionPA, videos	102
Table 54. Results: detectImpersonationPA, Stills vs. Videos	109
Table 55. Results: detectEvasionPA, Stills vs. Videos	123

List of Figures

Fig. 1. Scope of this report.	2
Fig. 2. Analog versus digital attacks	8
Fig. 3. DET Interpretation	14
Fig. 4. Bona Fide Still vs. Video Score Differences, Impersonation	25
Fig. 5. PA Still vs. Video Score Differences, Impersonation	26
Fig. 6. Error vs. Threshold, Still vs. Video, Impersonation	27
Fig. 7. Bona Fide Still vs. Video Score Differences, Evasion	29
Fig. 8. PA Still vs. Video Score Differences, Evasion	30
Fig. 9. Error vs. Threshold, Still vs. Video, Evasion	31
Fig. 10. BPCER by demographic, Impersonation	34
Fig. 11. BPCER by demographic, Evasion	35
Fig. 12. Appendix: DETs - detectImpersonationPA - stills	60
Fig. 13. Appendix: DETs - detectImpersonationPA - stills	61
Fig. 14. Appendix: DETs - detectImpersonationPA - stills	62
Fig. 15. Appendix: DETs - detectImpersonationPA - stills	63

Fig. 16.	Appendix: DETs - detectImpersonationPA - stills	64
Fig. 17.	Appendix: DETs - detectImpersonationPA - stills	65
Fig. 18.	Appendix: DETs - detectImpersonationPA - stills	66
Fig. 19.	Appendix: DETs - detectImpersonationPA - stills	67
Fig. 20.	Appendix: DETs - detectImpersonationPA - stills	68
Fig. 21.	Appendix: DETs - detectImpersonationPA - stills	69
Fig. 22.	Appendix: DETs - detectImpersonationPA - stills	70
Fig. 23.	Appendix: DETs - detectImpersonationPA - stills	71
Fig. 24.	Appendix: DETs - detectImpersonationPA - stills	72
Fig. 25.	Appendix: DETs - detectImpersonationPA - stills	73
Fig. 26.	Appendix: DETs - detectImpersonationPA - videos	74
Fig. 27.	Appendix: DETs - detectImpersonationPA - videos	75
Fig. 28.	Appendix: DETs - detectImpersonationPA - videos	76
Fig. 29.	Appendix: DETs - detectImpersonationPA - videos	77
Fig. 30.	Appendix: DETs - detectImpersonationPA - videos	78
Fig. 31.	Appendix: DETs - detectImpersonationPA - videos	79
Fig. 32.	Appendix: DETs - detectImpersonationPA - videos	80
Fig. 33.	Appendix: DETs - detectImpersonationPA - videos	81
Fig. 34.	Appendix: DETs - detectImpersonationPA - videos	82
Fig. 35.	Appendix: DETs - detectImpersonationPA - videos	83
Fig. 36.	Appendix: DETs - detectImpersonationPA - videos	84
Fig. 37.	Appendix: DETs - detectImpersonationPA - videos	85
Fig. 38.	Appendix: DETs - detectImpersonationPA - videos	86
Fig. 39.	Appendix: DETs - detectImpersonationPA - videos	87
Fig. 40.	Appendix: DETs - detectEvasionPA - stills	103
Fig. 41.	Appendix: DETs - detectEvasionPA - stills	104
Fig. 42.	Appendix: DETs - detectEvasionPA - stills	105
Fig. 43.	Appendix: DETs - detectEvasionPA - videos	106
Fig. 44.	Appendix: DETs - detectEvasionPA - videos	107
Fig. 45.	Appendix: DETs - detectEvasionPA - videos	108
Fig. 46.	Error Vs. Threshold Detection for Impersonation PA	112
Fig. 47.	Error Vs. Threshold Detection for Impersonation PA	113
Fig. 48.	Error Vs. Threshold Detection for Impersonation PA	114
Fig. 49.	Error Vs. Threshold Detection for Impersonation PA	115
Fig. 50.	Error Vs. Threshold Detection for Impersonation PA	116
Fig. 51.	Error Vs. Threshold Detection for Impersonation PA	117
Fig. 52.	Error Vs. Threshold Detection for Impersonation PA	118
Fig. 53.	Error Vs. Threshold Detection for Impersonation PA	119
Fig. 54.	Error Vs. Threshold Detection for Impersonation PA	120
Fig. 55.	Error Vs. Threshold Detection for Impersonation PA	121
Fig. 56.	Error Vs. Threshold Detection for Impersonation PA	122
Fig. 57.	Error Vs. Threshold Detection for Evasion PA	124
Fig. 58.	Error Vs. Threshold Detection for Evasion PA	125
Fig. 59.	Error Vs. Threshold Detection for Evasion PA	126
Fig. 60.	Error Vs. Threshold Detection for Evasion PA	127

Fig. 61. Race and Sex Demographic Barcharts for Impersonation PA	129
Fig. 62. Race and Sex Demographic Barcharts for Impersonation PA	130
Fig. 63. Race and Sex Demographic Barcharts for Impersonation PA	131
Fig. 64. Race and Sex Demographic Barcharts for Impersonation PA	132
Fig. 65. Race and Sex Demographic Barcharts for Impersonation PA	133
Fig. 66. Race and Sex Demographic Barcharts for Impersonation PA	134
Fig. 67. Race and Sex Demographic Barcharts for Impersonation PA	135
Fig. 68. Race and Sex Demographic Barcharts for Impersonation PA	136
Fig. 69. Race and Sex Demographic Barcharts for Impersonation PA	137
Fig. 70. Race and Sex Demographic Barcharts for Evasion PA	139
Fig. 71. Race and Sex Demographic Barcharts for Evasion PA	140
Fig. 72. Race and Sex Demographic Barcharts for Evasion PA	141

Executive Summary

Overview

This report documents the ability of software-based algorithms (software only, no hardware solutions) to detect the presence of presentation attacks in conventional 2D still and video imagery of human faces. For 82 prototype algorithms from 45 developers, the report surveys the trade-off between false alarm rates on legitimate non-attack images and detection rates on images of various presentation attack instruments (PAIs). All PAIs are detailed in the public domain, such that developers could have implemented defenses against them. The study was executed offline using archived images sequestered at NIST. It did not evaluate approaches based on 3D, near-infrared illumination, nor those based on real-time human interaction with a camera including challenge-response, variable illumination, and automated adjustment of the imaging system.

Motivation

As face recognition algorithms become ever more capable, they have been employed in remote enrollment and authentication applications in which the capture is not supervised by a trusted attendant. In such settings, an attacker can present arbitrarily modified faces to a camera. This is done either with the intent of *impersonation* of another person (e.g., fraudulent bank account access) or *evasion* in which the user is trying to not be recognized (e.g., entering a casino). Accordingly, the ISO/IEC 30107[1] series of standards define a presentation attack (PA) as “the presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy”. The standards also establish requirements on evaluations of PA detection approaches and metrics to summarize their accuracy.

Notable Observations and Results

PAD accuracy varies widely across algorithms, use cases (impersonation vs. evasion), and PA types. The detection of some PA types - photo print/replay attacks, protective face masks, and flexible silicon face masks - is well supported across multiple developers, while other PA types generated high detection error rates with all tested implementations. Many algorithms generate lower error rates when the input imagery is a video sequence when compared to a single still image from the same collection event. Additionally, by applying simple sum-rule fusion of PAD scores across multiple algorithms, the outcomes from fusion outperformed the top performing algorithm in all impersonation PA categories and in most evasion PA categories. A more detailed summary of results follows in the Technical Summary.

Technical Summary

Who Should Read This Report

This report covers PAD capabilities for **software-based** detection of **physical attacks** presented to the camera, without any interaction with the user or the hardware sensor. In short, algorithms are provided with a pre-existing image or video and make a PAD determination based solely on the information in the input imagery. As such, this report does not assess capabilities of hardware-enabled mechanisms that can alter optics or illumination during capture. Additionally it is silent on non-presentation attacks - e.g. those that subvert operation of software post-capture including injection attacks. Nevertheless passive, software-based PAD has a role in those applications where a commodity or non-biometric camera is used for collection of an image that is then transmitted to a receiving system. For example, if a passport photo is collected in a retail outlet using a generic portrait camera, the passport issuer may check for presentation attack.

Likewise in some countries' border control points, the capture subsystem may not include a (hardware) PAD module, instead relying on remote server-side PAD operating solely on the image. While software-based PAD is relevant in some operational settings, it only represents a small part of a much larger presentation attack technology landscape. Figure 1 guides readers in the relevance of this report.

What We Did

The NIST Information Technology Laboratory (ITL) quantified the accuracy of passive, software-based face presentation attack detection (PAD) algorithms applied to imagery of different presentation attack instruments (PAI). FATE PAD was open for participation worldwide between January 3rd, 2023 to February 28th, 2023, and developers were allowed to submit up to two algorithms for evaluation. Feedback in the form of algorithm report cards was provided to developers after each algorithm completed the trials. FATE PAD had two separate tasks that evaluated algorithms with an ability to detect 1) impersonation attacks and 2) evasion attacks. Developers could submit algorithms to one or both tasks. NIST evaluated 82

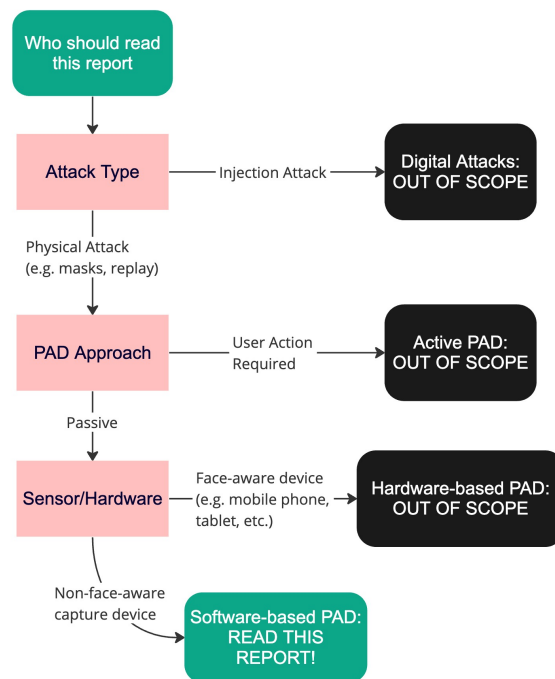


Fig. 1. Scope of this report.

algorithms from 45 unique developers worldwide. All algorithms implemented the impersonation detection task, and 27 of those algorithms also implemented the evasion detection task.

Our evaluation dataset contained imagery (primarily stills) of approximately 20 000 PA attempts and 21 000 bona fide presentations, which included 9 categories of PAs. The attacks used in this test are documented in the public domain. For PA types tested where detection appears to be well-supported by multiple developers, the PA descriptions are disclosed. For the remaining PA types, detection metrics are reported but without the name or description of the attack instrument.

How We Stated Performance

We used the PA attempts to estimate the Attack Presentation Classification Error Rate (APCER) or PA miss rate. We used the bona fide presentations to estimate the Bona Fide Presentation Classification Error Rate (BPCER) or false detection rate.

BPCER can be interpreted as the rate of inconvenience for legitimate users of the system whose presentation is being incorrectly detected as a PA. The consequence of such false detections is additional resources required to adjudicate the bona fide sample or unnecessary re-attempts or re-collection of the biometric sample. Conversely, APCER is the rate that fraud successfully takes place when a PA is incorrectly classified as a legitimate, bona fide sample. BPCER often gives a statement of the convenience of a system while APCER represents the security of a system.

The metrics are defined in the ISO/IEC 30107-3[2] standard. As in other decision systems, the two error rates can be traded off against each other - one goes up, the other goes down - by changing a decision threshold. The report includes figures showing this tradeoff and also two summary measures:

- ▷ **APCER @ BPCER = 0.01**, a convenience-focused metric that reports the proportion of undetected PAs when the false detection rate is limited to 1% of bona fide imagery. The approach of controlling BPCER (by setting an appropriate threshold) is important in those applications where the system owner cannot tolerate high rejection rates of legitimate bona-fide submissions, and when the attendant costs of undetected fraud are not punitive or if a priori PA-based fraud is rare (e.g., eGate operations).
- ▷ **BPCER @ APCER = 0.01**, a security-focused metric that reports the proportion of bona fide images incorrectly flagged as PAs when the PA miss rate is limited to 1% of PA imagery. The approach of controlling APCER by setting a threshold sufficient to detect a majority of PAs is important in those applications where rejection of bona-fide submissions is acceptable and when fraud costs associated with PA presentation are large (e.g., bank account access).

What We Found

Detection Performance: PAD performance varied widely across algorithms, use cases, and PA types, with only a small percentage of algorithms evaluated demonstrating notable detection capabilities. Tables 1 and 2 tabulate the top performing algorithm results for each PA type tested under the impersonation and evasion tasks, respectively.

PA types where detection appears to be well-supported by multiple developers (for either impersonation or evasion) are disclosed in the description column. For the remaining PA types, detection metrics for each PAI are reported but without description of the actual PAI.
Section 5.1

Table 1. Top Performers - Use Case: detectImpersonationPA - Media Type: stills

PA Type	Description	Algorithm	(Convenience) APCER @ BPCER=0.01	Algorithm	(Security) BPCER @ APCER=0.01
PA Type 1		kakao-001	0.07	iproov-000	0.069
PA Type 3	Flexible Silicone Face Mask	stcon-001	0.0	stcon-001	0.0003
PA Type 4		cyberlink-002	0.13	aware-001	0.200
PA Type 7		cyberlink-002	0.012	cyberlink-002	0.012
PA Type 8	Photo Print/Replay Attack	alice-001 idemia-011 idrnd-000 idrnd-001	0.0	idrnd-001	0.0001
PA Type 8 (zoomed)	Photo Print/Replay Attack (zoomed)	idrnd-001	0.005	idrnd-001	0.006

Table 2. Top Performers - Use Case: detectEvasionPA - Media Type: stills

PA Type	Description	Algorithm	(Convenience) APCER @ BPCER=0.01	Algorithm	(Security) BPCER @ APCER=0.01
PA Type 1		kakao-001	0.13	kakao-001	0.151
PA Type 2		kakao-001	0.12	alice-000	0.035
PA Type 3	Flexible Silicone Face Mask	onfido-000	0.05	alice-000	0.014
PA Type 4		kasikornlabs-000	0.62	aware-001	0.191
PA Type 5		kakao-001	0.0	kakao-001	0.0005
PA Type 6	Protective Face Mask	rankone-000 rankone-001	0.0	rankone-000	0.000
PA Type 7		kakao-001	0.14	cyberlink-002	0.035
PA Type 8	Photo Print/Replay Attack	kakao-000	0.009	kakao-000	0.006
PA Type 8 (zoomed)	Photo Print/Replay Attack (zoomed)	onfido-001	0.06	kakao-001	0.052

PA Type 9	kasikornlabs-000	0.052	cyberlink-002	0.028
-----------	------------------	-------	---------------	-------

Performance across PA Types: The detection of some PA types (i.e., photo print/replay attacks, protective face masks, and flexible silicone face masks) appears to be well supported by multiple developers, with relatively low error rates ($APCER \leq 0.01$ @ $BPCER=0.01$ and $BPCER \leq 0.01$ @ $APCER=0.01$) achieved by multiple developers. There are some PAs where detection is supported by only a limited number of developers (e.g., PA Type 7) and in some cases, by only a single developer (e.g., PA Type 5). However, there remain a number of PAs evaluated where detection error rates are high across all algorithms tested, indicative that some PAs still pose a threat to passive, software-based PAD approaches. *Section 5*

Photo Print/Replay Attacks: Detection of photo print/replay attacks where the frame of the printed photo/electronic tablet and the subject's hands are visible is well supported by multiple developers. However, when the view is zoomed in such that the frame of the printed photo/electronic tablet and the subject's hands are not visible, detection error rates increase across all algorithms, and in some cases, quite significantly. *Section 5*

Still vs. Video Imagery: A number of algorithms generate improved error rates when the input imagery is a video sequence when compared to a single still image from the same collection event. The existence and extent of PAD error reduction in videos versus stills is highly algorithm-dependent. *Section 5.3*

Fusion: We investigated to what extent fusion of multiple PAD algorithms might improve detection outcomes. Using simple sum-rule fusion of PAD scores from four more accurate algorithms applied to the same image, the accuracy of the combined algorithm exceeded that of the top performing algorithm in all impersonation PA categories and in most evasion PA categories. *Section 5.4*

Demographic Effects: While demographic effects was not a primary evaluation objective, first-order analysis of results was conducted on bona fide imagery to assess whether false detection rates (BPCER) vary across the race and sex groups represented in the test data. We analyzed BPCER for different race-sex groups at a fixed threshold that gave BPCER equal (or closest) to 0.03 on white males. False detection results across demographic groups varied across algorithms, and no obvious trends were observed in terms of elevated false detection rates isolated to a particular demographic group. *Section 5.5*

Impersonation vs. Evasion Results: PAD implementations are often fielded in applications where the classes of risk are known. For example, in authentication, a primary concern is impersonation. In background checks, the concern is of evasion/concealment. Presentation attack detection with the intent of impersonation vs. evasion was implemented and evaluated as separate functions. PAs used to evaluate impersonation detection were also used to test evasion detection on the basis that successful impersonation would also

constitute evasion. When tested on the same PAs, algorithms looking for the presence of impersonation generally performed better than those detecting evasion. For algorithms that implemented both impersonation and evasion detection functions, differences in error rates were also observed when tested on the same PAs for the same algorithm. This is evidence that the different functions are potentially targeting specific types of attacks.

Limitations

As our evaluation tested PAD capabilities under narrow conditions, this study doesn't fully capture the entire PAD technology landscape. Particularly the following points should be considered:

- ▷ **Digital attacks:** Digital “injection attacks” that feature a direct electronic introduction of a digital image or video, while an important aspect of the presentation attack landscape, were not evaluated.
- ▷ **Hardware-based PAD:** If PAD is deployed on a face-aware device (e.g., mobile device), there are opportunities to employ more sophisticated hardware-based PAD approaches that involve other sensors (e.g. time-of-flight), other illuminants (e.g. near infrared), other non-standardized data (e.g. lip movement) or signals sensed by the hardware (e.g., flashing lights). Our study did not evaluate hardware-based PAD approaches.
- ▷ **Active PAD:** In applications where the user is able to interact with the system in real-time, some PAD implementations can require the user to perform certain actions to prove their “liveness” such as asking the user to blink or turn their head. Such active challenge-response PAD approaches were not evaluated in our study.

1. Presentation Attack Detection (PAD)

1.1. Introduction

A presentation attack (PA), as defined by the ISO/IEC 30107[1] standard on biometric presentation attack detection, is "the presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy". A presentation attack is often launched with the intent of *impersonation* (the user is trying to authenticate as a target identity) or *evasion* (the user is trying to fool the biometric system into not recognizing their true identity). The goals of impersonation include trying to gain positive access privilege as someone else, for example, trying to unlock someone's cell phone or gain access to a facility. The goals of evasion are typically to conceal one's true identity to evade recognition from say a watchlist, or to create a separate enrollment under a different name. Biometric systems can be attacked by any of an open-ended set of presentation attack instruments, the number and type of which is determined by the effort and ingenuity of the attacker and the countermeasures instituted by the developer. Some examples of known presentation attack instruments include artificial "gummy" fingers[3], "replay" attacks where the attacker is holding a photo or video of someone's face to the camera, and iris photo and contact lens attacks.

Presentation attack of face recognition systems and the mechanisms to detect it are areas of high interest given the widespread deployment of face recognition systems, particularly in unmanned and unsupervised scenarios such as online remote enrollment and authentication.

1.2. Scope

1.2.1. Physical (Analog) vs. Digital Attacks

Presentation attacks are defined to include creation and introduction of physical artefacts to the sensor in the analog domain. Examples of this include donning a silicone face mask or holding up a printed photo or tablet display to the camera. As presentation attack methods evolve, attackers will also work to exploit weaknesses in the implementation after the sensor i.e., in the digital domain. These "injection attacks" feature a direct electronic introduction of a digital image or video. These are recently of particular concern in personal devices where a virtual camera is not readily distinguishable from the physical camera. This is a possibility in those scenarios where the capture cannot be trusted - for example in some mobile phones - because the integrity of the sensor/camera cannot be guaranteed. The FATE PAD activity evaluated physical attacks with analog artifacts. Digital injection attacks, while an important aspect of the presentation attack landscape, are out of scope for this evaluation.

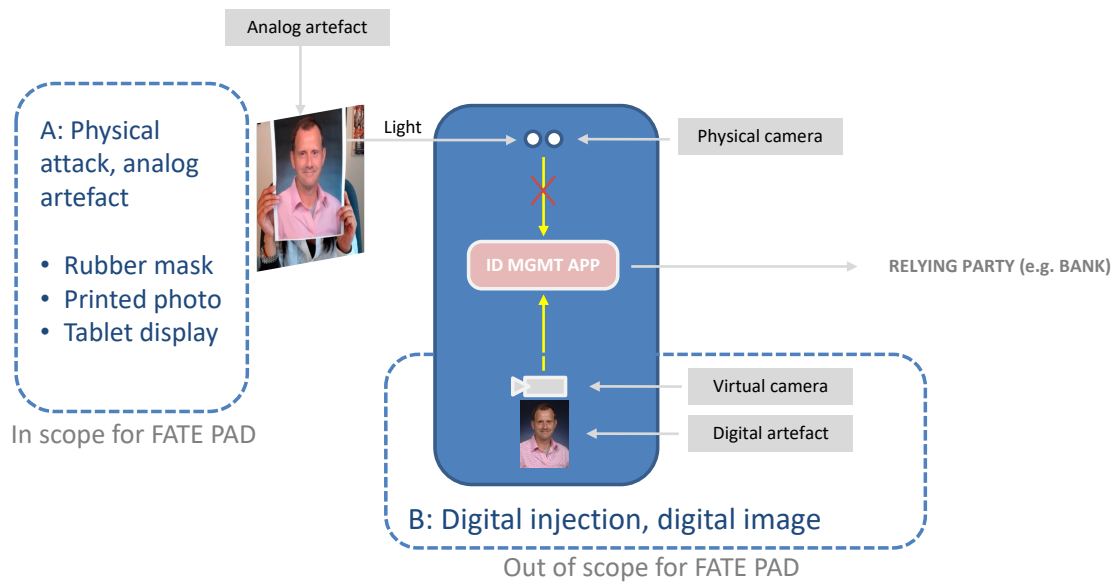


Fig. 2. Analog versus digital attacks

1.2.2. Passive PAD Approaches vs. User Interaction Required PAD

In applications where the user is able to interact with the system in real-time, some PAD implementations require the user to perform certain actions to prove their "liveness" such as asking the user to blink or turn their head. These are challenge-response approaches in which an attacker must emulate the expected response to the challenge.

However, in scenarios where user interaction is not possible and the PAD system can only operate on captured imagery (often without the user's awareness), this is known as passive PAD. In this test, we evaluated passive PAD approaches that operated on pre-collected imagery without any sort of user interaction. PAD approaches that require user interaction are out of scope for FATE PAD.

1.2.3. Software vs. Hardware-based PAD

PAD capabilities generally fall into two categories – software-based and hardware-based PAD. Table 3 summarizes the relevance and applications of software vs. hardware-based PAD. The FATE PAD activity provided independent testing of software-based facial PAD detection technologies. The evaluation is designed to assess *software-based* PAD detection capability to inform developers and current and prospective end-users. Software-based PAD solutions operate only on the captured imagery. Hardware-based PAD solutions are out of scope for FATE PAD.

Software-based PAD has a role in those applications where a commodity or non-biometric camera is used for collection of an image that is then transmitted to a receiving system. For example, if a passport or other ID photo is collected in a retail outlet using a generic portrait camera, the passport issuing agency may check for PA. Likewise in some countries' border control points, the capture subsystem may not include a (hardware) PAD module, instead relying on remote server-side PAD operating solely on the image.

	Software-based PAD	Hardware-based PAD
Input	Image/video	Image/video and other non-standardized data or signals sensed by dedicated hardware (e.g., flashing lights)
Mode of operation	Server-based or cloud-based PAD with non-face-aware capture device; offline PAD in existing/legacy systems	Client or edge-based PAD with dedicated face-aware capture device
Applications	Applications where capture processes and devices are not controlled or cannot be configured to perform PAD	Applications where hardware is controllable/configurable during the capture process to perform PAD

Table 3. Software vs. hardware-based PAD

1.2.4. Offline Testing

FATE PAD was conducted as an offline evaluation at a NIST facility by applying algorithms to still photos and video frames that are sequestered on computers controlled by NIST. Offline evaluations are attractive, because they allow uniform, fair, repeatable, and large-scale statistically robust testing. However, they do not capture all aspects of an operational system. Offline tests do not include a live image acquisition component or any interaction with real users. Our approach is adopted to allow evaluation on large datasets and to achieve repeatability where all algorithms are tested against the same evaluation datasets. Testing was performed on high-end server-class blades running the Ubuntu Linux [4] operating system. The test harness used concurrent processing to distribute workload across dozens of computers.

2. Datasets

The Presentation Attack Instruments (PAI) used in this test are documented in the public domain. Due to data sensitivities, our intention was to not disclose the PAIs used in our evaluation. This was intended to encourage broad PAD effectiveness across unknown PAs and to discourage tuning to specific attacks. This reflects the operational reality that

attackers don't advertise their methods. However, after evaluation of current PAD capabilities, we have decided to disclose a subset of the PA types where detection appears to be well-supported by multiple developers. For the remaining PA types, detection metrics for each PAI are reported but without the name or description of the PAI. PAs used to evaluate impersonation detection were also used to test evasion detection, because by definition, impersonation is also a form of evasion (by trying to look like someone else, you're also trying to not look like yourself). See Tables 4, 5, and 6.

Table 4. Dataset - Bona Fides

Description	Media Type	Num. Media
Bona Fide	stills	21218
Bona Fide	videos	538

Table 5. Dataset - Use Case: detectImpersonationPA

Label	Description	Media Type	Num. Media
PA Type 1		stills	1119
PA Type 3	Flexible Silicon Face Mask	stills	207
PA Type 4		stills	619
PA Type 7		stills	4573
PA Type 8	Photo Print/Replay Attack	stills	1417
PA Type 8 (zoomed)	Photo Print/Replay Attack (zoomed)	stills	1417
PA Type 1		videos	15
PA Type 3	Flexible Silicone Face Mask	videos	10
PA Type 8	Photo Replay Attack	videos	54

Table 6. Dataset - Use Case: detectEvasionPA

Label	Description	Media Type	Num. Media
PA Type 1		stills	3310
PA Type 2		stills	105
PA Type 3	Flexible Silicon Face Mask	stills	207
PA Type 4		stills	619
PA Type 5		stills	256
PA Type 6	Protective Face Mask	stills	1209
PA Type 7		stills	4629
PA Type 8	Photo Print/Replay Attack	stills	1417
PA Type 8 (zoomed)	Photo Print/Replay Attack (zoomed)	stills	1417
PA Type 9		stills	6473
PA Type 1		videos	56
PA Type 3	Flexible Silicon Face Mask	videos	10

PA Type 5		videos	51
PA Type 8	Photo Replay Attack	videos	54
PA Type 9		videos	38

2.1. Description of Disclosed PAIs

Photo Print/Replay Attack: Imagery includes subjects presenting a printed photo or digital photo displayed on a high resolution electronic tablet to the camera. The frame of the printed photo/electronic tablet and the subject's hands are typically visible.

Photo Print/Replay Attack (zoomed): Imagery includes subjects presenting a printed photo or digital photo on a high resolution electronic tablet to the camera, zoomed in such that the frame of the printed photo/electronic tablet and the subject's hands are not visible.

Protective Face Mask: Imagery includes subjects wearing commonly-used protective face masks, including disposable surgical masks and solid and patterned fabric masks. Patterns on masks did not include any facial features.

Flexible Silicon Face Mask: Imagery includes subjects wearing flexible silicone whole-head face masks.

2.2. Description of Imagery

All imagery is collected with a color camera that is in a fixed position, and only color images and videos are used in the evaluation. Stills and videos contain a single, cooperative subject, with neutral expression, approximately centered in the field of view. Still image dimensions range from 640x480 to 5184x3456.

Video sequences are variable length across all samples provided. Videos only contain entirely bona fide attempts or entirely presentation attack attempts. The use of compression is operationally realistic for those applications where PAD operates on received media rather than a live-captured stream direct from the sensor. All videos in this test were compressed with h264, with compression ratios in the range of 30:1 to 50:1. Video frame rate was provided as input to the algorithm in frames per second (fps). Frame rates range from 24 fps to 60 fps, with typical frame rate of 24 frames per second. Video duration ranges from 3 seconds to 30 seconds, with typical duration of 25 seconds. Video frame width and height in pixels are provided to the algorithm. Video frame dimensions range from 1920x1080 (1080p) to 3840x2160 (4K).

3. Metrics

In this section, we adopt terminology from the presentation attack detection testing standard[2] to quantify PAD accuracy. Presentation attack detection requires submitted algorithms to determine whether a particular sample contains a presentation attack or not. Given an image or a video, algorithms reported 1) a binary decision on whether the sample contains a PA or not and 2) a confidence score on $[-1, 1]$ representing the algorithm's certainty about whether the sample is a PA $[+1]$ or not $[-1]$ or indeterminate $[0]$. A low score $[-1]$ indicates certainty that the media does not contain a PA, and a high score $[+1]$ represents certainty that the media does contain a PA.

This report computes and reports the following metrics:

3.1. Attack Presentation Classification Error Rate (APCER)

APCER is defined as the the proportion of presentation attack samples incorrectly classified as bona fide presentation

3.2. Bona Fide Presentation Classification Error Rate (BPCER)

BPCER is defined as the proportion of bona fide samples incorrectly classified as presentation attack samples

3.3. Failure to Process Events

Attack Presentation Non-Response Rate (APNRR) and Bona Fide Presentation Non-Response Rate (BPNRR) are defined as the proportion of presentation attack and bona fide samples, respectively, that do not generate a response and fail to be processed by the algorithm software, whether it's elective refusal to process the imagery or an involuntary error. Failure to process events are logged when the algorithm software returns a nonsuccessful return code from the PAD function, indicating that something went wrong while processing the imagery for PAD. ISO/IEC 30107-3[2] includes APNRR as "proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem" to quantify outcomes where the sensor is not even triggered by the presented PA sample. We use APNRR to quantify that for the PAD-subsystem, which here is the algorithm under test.

Failure to process events are incorporated into the calculation of BPCER and APCER. All occurrences of failure to process by an algorithm are treated as if a presentation attack is detected with the confidence score set to $+1$. This implements a failure-is-considered-suspicious policy.

3.4. Detection Error Tradeoff (DET)

We assess detection accuracy by analyzing the confidence score returned by the algorithm. In this case, the higher the confidence value, the more likely the algorithm thinks the sample contains a PA. A reasonable approach to the detection problem is to classify a sample as either a PA or bona fide sample by thresholding on its confidence value.

Given N detection scores on bona fide imagery, b , the BPCER is computed as the proportion above some threshold, T . Similarly, given P detection scores on PA imagery, p , the APCER is computed as the proportion below some threshold, T . $H(x)$ is the unit step function[5], and $H(0)$ is taken to be 1.

$$\text{BPCER}(T) = \frac{1}{N} \sum_{i=1}^N H(b_i - T), \quad (1)$$

$$\text{APCER}(T) = 1 - \frac{1}{P} \sum_{i=1}^P H(p_i - T). \quad (2)$$

Operationally, there are two primary types of errors to be considered for presentation attack detection - BPCER and APCER. BPCER, which gives an indication of how often a legitimate user of the system is inconvenienced as an incorrectly flagged attack. The consequence of such false detections is additional resources required to adjudicate the bona fide sample or unnecessary re-attempts or re-collection of the biometric sample. Conversely, APCER is the rate that fraud successfully takes place when a PA is incorrectly classified as a legitimate, bona fide sample. BPCER often gives a statement of the convenience of a system while APCER represents the security of a system.

In applications where large volumes of (presumably legitimate) transactions occur (e.g., eGate operations), a PAD system would typically be configured at thresholds to minimize BPCER or false detection rate. BPCER could be limited to some percentage that is commensurate with the amount of resources available to conduct secondary processes. We consider these *convenience-focused* use cases.

In applications where the focus is to minimize undetected presentation attacks (e.g., bank account access), then a PAD system might be configured at thresholds that are focused on minimizing APCER (or PA miss rate). We consider these *security-focused* use cases.

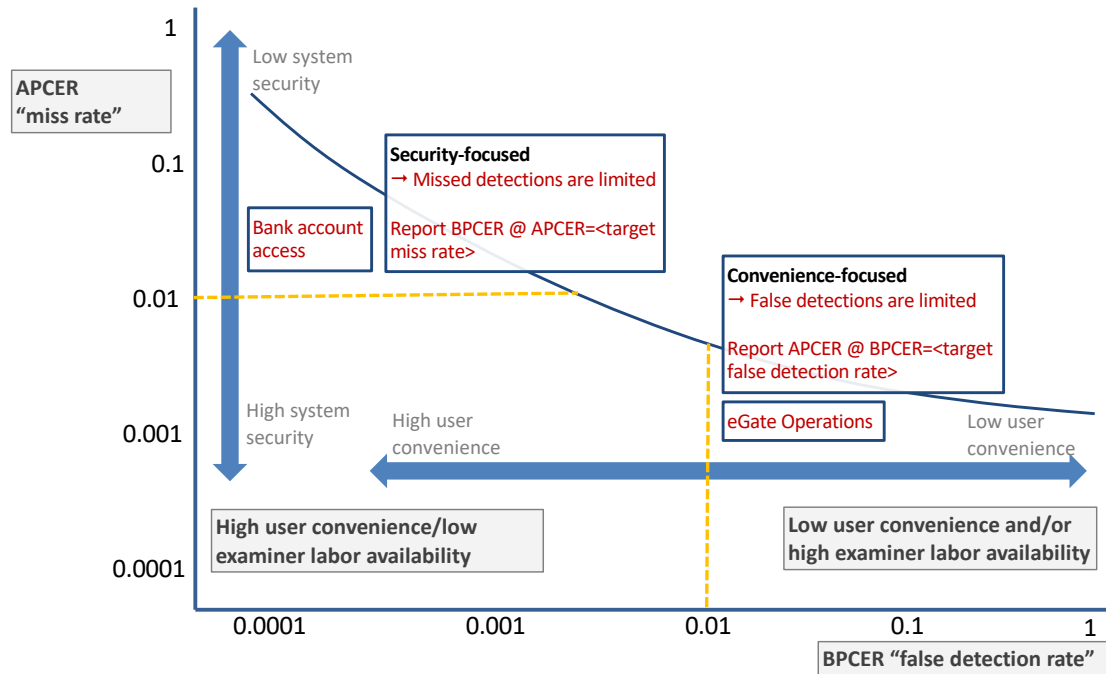


Fig. 3. Illustration of error tradeoff between misses and false detections.

There is typically a tradeoff between PA miss rates and false detection rates. Setting thresholds to minimize false detection rates will likely come at a cost of increased PA miss rates and vice versa. The results in this paper report the following:

- APCER @ BPCER = 0.01. Convenience-focused metric that reports the proportion of undetected PAs when the false detection rate is limited to 1% of bona fide imagery.
- BPCER @ APCER = 0.01. Security-focused metric that reports the proportion of bona fide images incorrectly flagged as PAs when the PA miss rate is limited to 1% of PA imagery.

4. Participation

The FATE PAD activity was open to participation worldwide between January 3rd, 2023 to February 28th, 2023. There was no charge to participate. Developers were allowed to submit up to two algorithms for evaluation. The process and format of algorithm submissions to NIST are described in the PAD Concept, Evaluation Plan, and API [6] document. Participants provided their submissions in the form of libraries compiled on a specific Linux kernel, which were linked against NIST’s test harness to produce executables. NIST provided a validation package to participants to ensure that NIST’s execution of submitted libraries produced the expected output on NIST’s test machines.

This report documents the results of algorithms submitted to FATE PAD for testing, and Table 7 lists the algorithms that were tested, in alphabetical order.

Table 7. Participant Information. This table presents the [participant location](#), organization name, algorithm name, and which PAD use cases were implemented.

	Loc.	Developer Name	Short Name	Impersonation	Evasion
1	KR	Alchera Inc	alchera-000	x	x
2	ES	Alice Biometrics	alice-000	x	x
3	ES	Alice Biometrics	alice-001	x	
4	US	Aware	aware-001	x	x
5	US	Aware	aware-002	x	x
6	IN	Biocube Matrics	biocube-001	x	
7	IN	Biocube Matrics	biocube-002	x	
8	KR	Cubox	cubox-000	x	x
9	KR	Cubox	cubox-001	x	x
10	TW	Cyberlink Corp	cyberlink-001	x	x
11	TW	Cyberlink Corp	cyberlink-002	x	x
12	US	Face Direct	facedirect-001	x	x
13	US	Face Direct	facedirect-002	x	x
14	ES	FacePhi	facephi-000	x	
15	ES	FacePhi	facephi-001	x	
16	US	Griaule	griaule-000	x	x
17	US	Griaule	griaule-001	x	x
18	MX	HuBOX	spooff-000	x	x
19	IN	HyperVerge Inc	hyperverge-001	x	
20	IN	HyperVerge Inc	hyperverge-002	x	
21	US	ID R&D	idrnd-000	x	
22	US	ID R&D	idrnd-001	x	
23	CL	ID Vision Ctr	idvisioncenter-001	x	
24	CL	ID Vision Ctr	idvisioncenter-002	x	
25	FR	ID3 Technology	id3-001	x	
26	FR	Idemia	idemia-010	x	
27	FR	Idemia	idemia-011	x	
28	SA	iiDENTIFIi	iiidentifi-000	x	
29	US	Incode Technologies Inc	incode-000	x	
30	US	Incode Technologies Inc	incode-001	x	
31	SK	Innovatrics	innovatrics-001	x	
32	SK	Innovatrics	innovatrics-002	x	
33	LU	Intema-LGL Group	intema-000	x	
34	LU	Intema-LGL Group	intema-001	x	
35	UK	iProov	iproov-000	x	
36	UK	iProov	iproov-001	x	
37	JP	Japan Computer Vision	jcv-001	x	x
38	JP	Japan Computer Vision	jcv-002	x	
39	KR	Kakao Brain	kakao-000	x	x
40	KR	Kakao Brain	kakao-001	x	x
41	TH	Kasikorn Labs	kasikornlabs-000	x	x
42	TH	Kasikorn Labs	kasikornlabs-001	x	x

Table 7. Participant Information. This table presents the [participant location](#), organization name, algorithm name, and which PAD use cases were implemented. (*continued*)

	Loc.	Developer Name	Short Name	Impersonation	Evasion
43	ES	Mobbeel Solutions	mobbl-000	x	
44	ES	Mobbeel Solutions	mobbl-001	x	
45	KZ	Modern Biometric Solutions	mbsolutions-000	x	
46	KZ	Modern Biometric Solutions	mbsolutions-001	x	
47	LT	Neurotechnology	neurotechnology-000	x	x
48	LT	Neurotechnology	neurotechnology-001	x	x
49	KR	NSENSE Korea	nsensekorea-000	x	
50	KR	NSENSE Korea	nsensekorea-001	x	
51	UK	Onfido	onfido-000	x	x
52	UK	Onfido	onfido-001	x	x
53	TW	PAPAGO Inc	papago-001	x	x
54	CH	PXL Vision AG	pxl-000	x	
55	CH	PXL Vision AG	pxl-001	x	
56	US	Rank One Computing	rankone-000	x	x
57	US	Rank One Computing	rankone-001	x	x
58	DE	Saffe	saffe-001	x	
59	DE	Saffe	saffe-002	x	
60	SA	STCON LLC	stcon-000	x	
61	SA	STCON LLC	stcon-001	x	
62	CH	Tech5 SA	tech5-001	x	
63	TR	Techsign	techsign-000	x	
64	TR	Techsign	techsign-001	x	
65	US	Trueface.ai	trueface-000	x	x
66	PT	Universidade de Coimbra	visteam-001	x	
67	PT	Universidade de Coimbra	visteam-002	x	
68	TW	UXLabs	uxlabs-001	x	x
69	ES	Veridas Digital Authentication Sol.	veridas-001	x	
70	ES	Veridas Digital Authentication Sol.	veridas-002	x	
71	KZ	Verigram	verigram-000	x	
72	KZ	Verigram	verigram-001	x	
73	ID	Verihubs	verihubs-inteligensia-000	x	
74	ID	Verihubs	verihubs-inteligensia-001	x	
75	ID	VIDA-Digital Identity Pte Ltd	vida-001	x	
76	ID	VIDA-Digital Identity Pte Ltd	vida-002	x	
77	CN	Vision Intelligence Ctr of Meituan	meituan-000	x	
78	CN	Vision Intelligence Ctr of Meituan	meituan-001	x	
79	PT	YooniK	yooniK-001	x	
80	PT	YooniK	yooniK-002	x	
81	UK	Yoti	yoti-001	x	
82	UK	Yoti	yoti-002	x	

5. Results

The results in this section summarize PAD performance for the top performing algorithms. A complete tabulation of performance results for all algorithms is documented in Appendix A. The number after the $\pm$ indicates uncertainty related to sample size - it spans 95% of bootstrap samples of the PA scores.

5.1. Impersonation

Table 8. PA Type 1 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	(Convenience)	Rank	Algorithm	(Security)	Rank
	APCER @ BPCER=0.01			BPCER @ APCER=0.01	
kakao-001	0.07 ± 0.01	1	iproov-000	0.069	1
idrnd-001	0.1 ± 0.02	2	idrnd-001	0.082	2
idrnd-000	0.12 ± 0.02	3	kakao-001	0.105	3
stcon-001	0.13 ± 0.02	4	idrnd-000	0.133	4
iproov-001	0.16 ± 0.02	5	cyberlink-002	0.207	5
cyberlink-002	0.18 ± 0.02	6	aware-001	0.308	6
kakao-000	0.31 ± 0.03	7	stcon-001	0.346	7
stcon-000	0.31 ± 0.03	7	kasikornlabs-000	0.348	8
cyberlink-001	0.42 ± 0.03	9	aware-002	0.356	9
onfido-000	0.47 ± 0.03	10	iproov-001	0.377	10

Table 9. PA Type 3 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	(Convenience)	Rank	Algorithm	(Security)	Rank
	APCER @ BPCER=0.01			BPCER @ APCER=0.01	
stcon-001	0 ± 0	1	stcon-001	0.000	1
stcon-000	0.005 ± 0.007	2	alice-001	0.004	2
alice-001	0.01 ± 0.01	3	stcon-000	0.006	3
cyberlink-002	0.01 ± 0.01	3	cyberlink-002	0.007	4
idrnd-001	0.02 ± 0.02	5	idrnd-001	0.012	5
incode-001	0.02 ± 0.02	5	alice-000	0.014	6
idrnd-000	0.03 ± 0.02	7	cyberlink-001	0.020	7
cyberlink-001	0.03 ± 0.02	7	iproov-000	0.021	8
onfido-000	0.05 ± 0.03	9	idrnd-000	0.027	9
iiidentifi-000	0.06 ± 0.03	10	onfido-000	0.036	10

Table 10. PA Type 4 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	(Convenience)	Rank	Algorithm	(Security)	Rank
	APCER @ BPCER=0.01			BPCER @ APCER=0.01	
cyberlink-002	0.13 ± 0.03	1	aware-001	0.200	1
cyberlink-001	0.18 ± 0.03	2	cyberlink-002	0.207	2
stcon-001	0.19 ± 0.03	3	iproov-000	0.315	3
stcon-000	0.29 ± 0.04	4	aware-002	0.322	4
idrnd-001	0.42 ± 0.04	5	idrnd-001	0.395	5
idrnd-000	0.47 ± 0.04	6	idrnd-000	0.395	5
meituan-001	0.53 ± 0.04	7	cyberlink-001	0.408	7
iproov-001	0.55 ± 0.04	8	vida-001	0.447	8
alice-001	0.56 ± 0.04	9	kasikornlabs-000	0.452	9
jcv-001	0.59 ± 0.04	10	intema-001	0.463	10

Table 11. PA Type 7 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	(Convenience)	Rank	Algorithm	(Security)	Rank
	APCER @ BPCER=0.01			BPCER @ APCER=0.01	
cyberlink-002	0.012 ± 0.003	1	cyberlink-002	0.012	1
cyberlink-001	0.052 ± 0.006	2	cyberlink-001	0.095	2
kakao-001	0.06 ± 0.007	3	kakao-001	0.159	3
alice-001	0.108 ± 0.009	4	onfido-001	0.263	4
kakao-000	0.16 ± 0.01	5	innovatrics-002	0.275	5
hyperverge-002	0.31 ± 0.01	6	veridas-002	0.291	6
veridas-002	0.32 ± 0.01	7	veridas-001	0.297	7
onfido-001	0.33 ± 0.01	8	alice-001	0.345	8
idrnd-000	0.33 ± 0.01	8	idrnd-000	0.348	9
idrnd-001	0.42 ± 0.01	10	idrnd-001	0.356	10

Table 12. PA Type 8 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	(Convenience)	Rank	Algorithm	(Security)	Rank
	APCER @ BPCER=0.01			BPCER @ APCER=0.01	
alice-001	0 ± 0	1	alice-001	0.000	1
idemia-011	0 ± 0	1	idrnd-000	0.000	1
idrnd-000	0 ± 0	1	idrnd-001	0.000	1
idrnd-001	0 ± 0	1	idemia-011	0.002	4
hyperverge-002	0.001 ± 0.001	5	hyperverge-002	0.003	5

kakao-001	0.001 ± 0.001	5	kakao-001	0.003	5
iproov-001	0.003 ± 0.002	7	meituan-001	0.003	5
meituan-001	0.004 ± 0.003	8	iproov-001	0.005	8
stcon-000	0.008 ± 0.005	9	kakao-000	0.005	8
hyperverge-001	0.008 ± 0.005	9	stcon-000	0.007	10

Table 13. PA Type 8 (zoomed) - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	(Convenience)		Algorithm	(Security)	
	APCER @ BPCER=0.01	Rank		BPCER @ APCER=0.01	Rank
idrnd-001	0.005 ± 0.004	1	idrnd-001	0.006	1
idrnd-000	0.011 ± 0.005	2	idrnd-000	0.010	2
stcon-000	0.018 ± 0.007	3	stcon-000	0.016	3
idemia-011	0.028 ± 0.009	4	idemia-011	0.026	4
kakao-001	0.031 ± 0.009	5	kakao-001	0.026	4
iproov-001	0.04 ± 0.01	6	jcv-002	0.039	6
jcv-001	0.05 ± 0.01	7	jcv-001	0.044	7
stcon-001	0.06 ± 0.01	8	meituan-001	0.045	8
onfido-001	0.06 ± 0.01	8	iproov-000	0.046	9
kakao-000	0.06 ± 0.01	8	iproov-001	0.047	10

5.2. Evasion

Table 14. PA Type 1 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience)		Algorithm	(Security)	
	APCER @ BPCER=0.01	Rank		BPCER @ APCER=0.01	Rank
kakao-001	0.13 ± 0.01	1	kakao-001	0.151	1
kakao-000	0.28 ± 0.02	2	cyberlink-002	0.254	2
rankone-000	0.39 ± 0.02	3	aware-002	0.418	3
rankone-001	0.39 ± 0.02	3	kasikornlabs-000	0.495	4
kasikornlabs-000	0.4 ± 0.02	5	aware-001	0.507	5
cyberlink-002	0.44 ± 0.02	6	alice-000	0.517	6
aware-002	0.51 ± 0.02	7	kasikornlabs-001	0.542	7
neurotechnology-000	0.53 ± 0.02	8	uxlabs-001	0.600	8
kasikornlabs-001	0.53 ± 0.02	8	kakao-000	0.635	9
onfido-000	0.55 ± 0.02	10	rankone-000	0.665	10

Table 15. PA Type 2 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience) APCER @ BPCER=0.01	Rank	Algorithm	(Security) BPCER @ APCER=0.01	Rank
kakao-001	0.12 ± 0.06	1	alice-000	0.035	1
onfido-000	0.17 ± 0.07	2	cyberlink-002	0.077	2
kakao-000	0.18 ± 0.07	3	kakao-001	0.108	3
aware-002	0.33 ± 0.09	4	aware-001	0.171	4
onfido-001	0.4 ± 0.1	5	aware-002	0.173	5
neurotechnology-000	0.4 ± 0.1	5	onfido-000	0.221	6
cyberlink-002	0.4 ± 0.1	5	neurotechnology-000	0.297	7
kasikornlabs-000	0.5 ± 0.1	8	kakao-000	0.315	8
kasikornlabs-001	0.6 ± 0.1	9	cyberlink-001	0.361	9
facedirect-002	0.64 ± 0.09	10	kasikornlabs-001	0.386	10

Table 16. PA Type 3 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience) APCER @ BPCER=0.01	Rank	Algorithm	(Security) BPCER @ APCER=0.01	Rank
onfido-000	0.05 ± 0.03	1	alice-000	0.014	1
onfido-001	0.09 ± 0.04	2	onfido-000	0.036	2
aware-002	0.1 ± 0.04	3	cyberlink-002	0.041	3
facedirect-002	0.16 ± 0.05	4	onfido-001	0.051	4
neurotechnology-000	0.26 ± 0.06	5	aware-001	0.052	5
kasikornlabs-000	0.26 ± 0.06	5	aware-002	0.057	6
kasikornlabs-001	0.29 ± 0.06	7	neurotechnology-000	0.197	7
kakao-001	0.57 ± 0.07	8	kasikornlabs-000	0.251	8
cyberlink-002	0.6 ± 0.07	9	neurotechnology-001	0.297	9
kakao-000	0.68 ± 0.06	10	kasikornlabs-001	0.329	10

Table 17. PA Type 4 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience) APCER @ BPCER=0.01	Rank	Algorithm	(Security) BPCER @ APCER=0.01	Rank
kasikornlabs-000	0.62 ± 0.04	1	aware-001	0.191	1
kasikornlabs-001	0.62 ± 0.04	1	aware-002	0.348	2
cyberlink-002	0.63 ± 0.04	3	cyberlink-002	0.446	3
onfido-001	0.74 ± 0.03	4	kasikornlabs-000	0.452	4
aware-002	0.76 ± 0.03	5	kasikornlabs-001	0.555	5

kakao-001	0.82 ± 0.03	6	onfido-001	0.621	6
onfido-000	0.82 ± 0.03	6	onfido-000	0.788	7
kakao-000	0.89 ± 0.03	8	alice-000	0.813	8
facedirect-001	0.9 ± 0.02	9	kakao-001	0.815	9
cubox-001	0.9 ± 0.02	9	neurotechnology-001	0.883	10

Table 18. PA Type 5 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience)		Rank	Algorithm	(Security)		Rank
	APCER @				BPCER @		
	BPCER=0.01				APCER=0.01		
kakao-001	0 ± 0	1		kakao-001	0.001	1	
kakao-000	0.02 ± 0.01	2		kakao-000	0.034	2	
cyberlink-002	0.34 ± 0.06	3		uxlabs-001	0.207	3	
facedirect-002	0.44 ± 0.06	4		aware-002	0.390	4	
aware-002	0.65 ± 0.06	5		aware-001	0.495	5	
griaule-000	0.68 ± 0.06	6		spooff-000	0.497	6	
rankone-000	0.73 ± 0.05	7		cyberlink-002	0.560	7	
rankone-001	0.73 ± 0.05	7		rankone-000	0.665	8	
onfido-001	0.79 ± 0.05	9		rankone-001	0.665	8	
onfido-000	0.82 ± 0.04	10		papago-001	0.696	10	

Table 19. PA Type 6 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience)		Rank	Algorithm	(Security)		Rank
	APCER @				BPCER @		
	BPCER=0.01				APCER=0.01		
rankone-000	0 ± 0	1		rankone-000	0.000	1	
rankone-001	0 ± 0	1		rankone-001	0.000	1	
trueface-000	0.002 ± 0.002	3		trueface-000	0.003	3	
kakao-000	0.008 ± 0.005	4		kakao-000	0.004	4	
cyberlink-002	0.012 ± 0.006	5		cyberlink-002	0.011	5	
kakao-001	0.014 ± 0.007	6		kakao-001	0.012	6	
neurotechnology-000	0.21 ± 0.02	7		aware-001	0.038	7	
griaule-001	0.34 ± 0.03	8		aware-002	0.053	8	
griaule-000	0.49 ± 0.03	9		cyberlink-001	0.119	9	
aware-002	0.51 ± 0.03	10		uxlabs-001	0.133	10	

Table 20. PA Type 7 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience) APCER @ BPCER=0.01	Rank	Algorithm	(Security) BPCER @ APCER=0.01	Rank
kakao-001	0.14 ± 0.01	1	cyberlink-002	0.035	1
kakao-000	0.15 ± 0.01	2	kakao-001	0.202	2
onfido-001	0.34 ± 0.01	3	onfido-001	0.284	3
onfido-000	0.43 ± 0.01	4	alice-000	0.377	4
rankone-000	0.52 ± 0.01	5	aware-002	0.473	5
rankone-001	0.52 ± 0.01	5	uxlabs-001	0.495	6
cyberlink-002	0.52 ± 0.01	5	neurotechnology-000	0.525	7
neurotechnology-000	0.65 ± 0.01	8	kakao-000	0.574	8
aware-002	0.8 ± 0.01	9	rankone-000	0.607	9
kasikornlabs-000	0.84 ± 0.01	10	rankone-001	0.607	9

Table 21. PA Type 8 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience) APCER @ BPCER=0.01	Rank	Algorithm	(Security) BPCER @ APCER=0.01	Rank
kakao-000	0.009 ± 0.005	1	kakao-000	0.006	1
onfido-001	0.017 ± 0.007	2	kakao-001	0.013	2
kakao-001	0.018 ± 0.007	3	alice-000	0.015	3
onfido-000	0.024 ± 0.008	4	onfido-000	0.019	4
aware-002	0.08 ± 0.01	5	onfido-001	0.020	5
kasikornlabs-000	0.09 ± 0.01	6	cyberlink-002	0.067	6
neurotechnology-000	0.1 ± 0.02	7	aware-002	0.075	7
kasikornlabs-001	0.15 ± 0.02	8	neurotechnology-000	0.095	8
facedirect-002	0.47 ± 0.03	9	kasikornlabs-000	0.126	9
cyberlink-002	0.51 ± 0.03	10	kasikornlabs-001	0.141	10

Table 22. PA Type 8 (zoomed) - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience) APCER @ BPCER=0.01	Rank	Algorithm	(Security) BPCER @ APCER=0.01	Rank
onfido-001	0.06 ± 0.01	1	kakao-001	0.052	1
onfido-000	0.07 ± 0.01	2	onfido-001	0.096	2
kakao-000	0.07 ± 0.01	2	kakao-000	0.099	3
kakao-001	0.12 ± 0.02	4	onfido-000	0.219	4
kasikornlabs-000	0.12 ± 0.02	4	neurotechnology-001	0.224	5

kasikornlabs-001	0.22 ± 0.02	6	aware-002	0.329	6
facedirect-002	0.3 ± 0.02	7	kasikornlabs-000	0.574	7
neurotechnology-000	0.3 ± 0.02	7	kasikornlabs-001	0.628	8
aware-002	0.31 ± 0.02	9	uxlabs-001	0.628	8
facedirect-001	0.83 ± 0.02	10	papago-001	0.696	10

Table 23. PA Type 9 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	(Convenience)	Rank	Algorithm	(Security)	Rank
	APCER @ BPCER=0.01			BPCER @ APCER=0.01	
kasikornlabs-000	0.052 ± 0.005	1	cyberlink-002	0.027	1
kasikornlabs-001	0.063 ± 0.006	2	alice-000	0.034	2
onfido-000	0.068 ± 0.006	3	kasikornlabs-000	0.055	3
kakao-001	0.107 ± 0.007	4	aware-001	0.066	4
onfido-001	0.135 ± 0.008	5	kasikornlabs-001	0.095	5
kakao-000	0.25 ± 0.01	6	onfido-000	0.146	6
rankone-000	0.27 ± 0.01	7	aware-002	0.161	7
rankone-001	0.27 ± 0.01	7	onfido-001	0.195	8
aware-002	0.34 ± 0.01	9	uxlabs-001	0.200	9
cyberlink-002	0.41 ± 0.01	10	kakao-001	0.242	10

5.3. Stills vs. Videos

The evaluation dataset contained 747 videos (538 bona fide, 209 PA). For each video collected, there was also a corresponding still image captured from the same collection event. This allows for the comparison of PAD performance when the input media is a video sequence or a single still image.

5.3.1. Impersonation

There were a total of 538 bona fide videos and corresponding stills and 79 impersonation PA videos and corresponding stills across 3 different PA types. DET analysis was conducted using all 79 PA imagery collections and 538 bona fide imagery collections. Table 24 tabulates performance results by still vs. video imagery. Individual PAD performance with videos for each PA type is available in Appendix A.2.

Table 24. Use Case: detectImpersonationPA - Stills vs. Videos

(Convenience)	(Security)
APCER @	BPCER @
BPCER=0.01	APCER=0.01

Algorithm	Stills	Videos	Algorithm	Stills	Videos
cyberlink-002	0.00	0.00	cyberlink-002	0.00	0.01
stcon-001	0.03	0.01	stcon-001	0.05	0.01
cyberlink-001	0.03	0.03	kasikornlabs-000	0.19	0.02
idrnd-001	0.05	0.03	cyberlink-001	0.03	0.03
iproov-001	0.05	0.03	iproov-000	0.05	0.03
stcon-000	0.09	0.03	idrnd-001	0.07	0.03
idrnd-000	0.08	0.04	kakao-001	0.07	0.05
kakao-001	0.01	0.04	kasikornlabs-001	0.25	0.06
kasikornlabs-000	0.10	0.04	hyperverge-002	1.00	0.07
alice-001	0.12	0.06	iproov-001	0.05	0.07

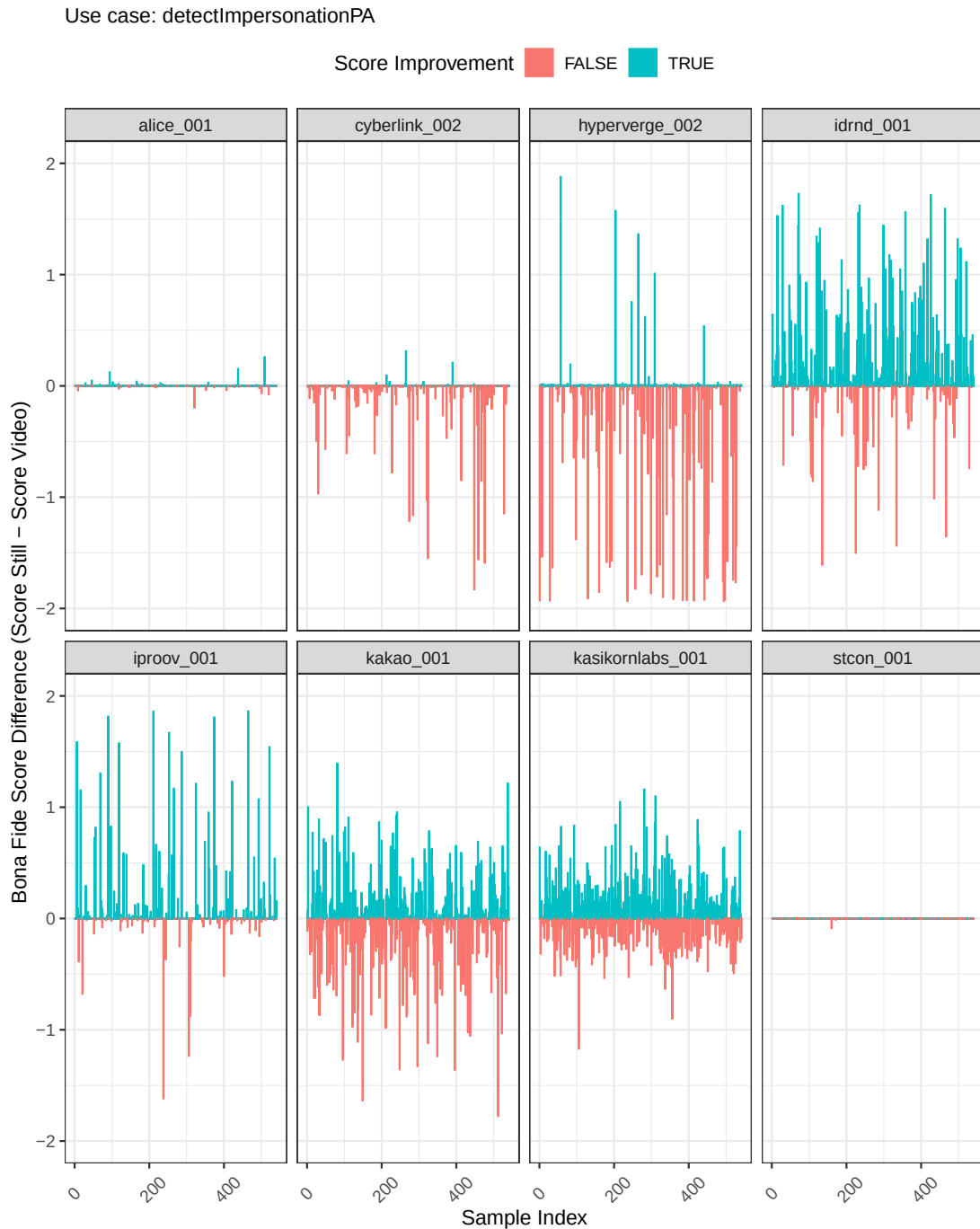


Fig. 4. This plot presents 1) pairwise bona fide PAD score differences between still and video scores of the same collection event and 2) whether or not a video sequence of the same collection event yields improvements over a single still image for better bona fide prediction outcomes. Teal colored lines represent improvement in bona fide PAD scores when a video is provided as input (vs. a still image), and the length of the line represents the magnitude of improvement (longer lines mean more improvement). Red lines indicate degradation of bona fide PAD scores with video input (vs. still), which means bona fide prediction degrades when the input is a video when compared to a still image.

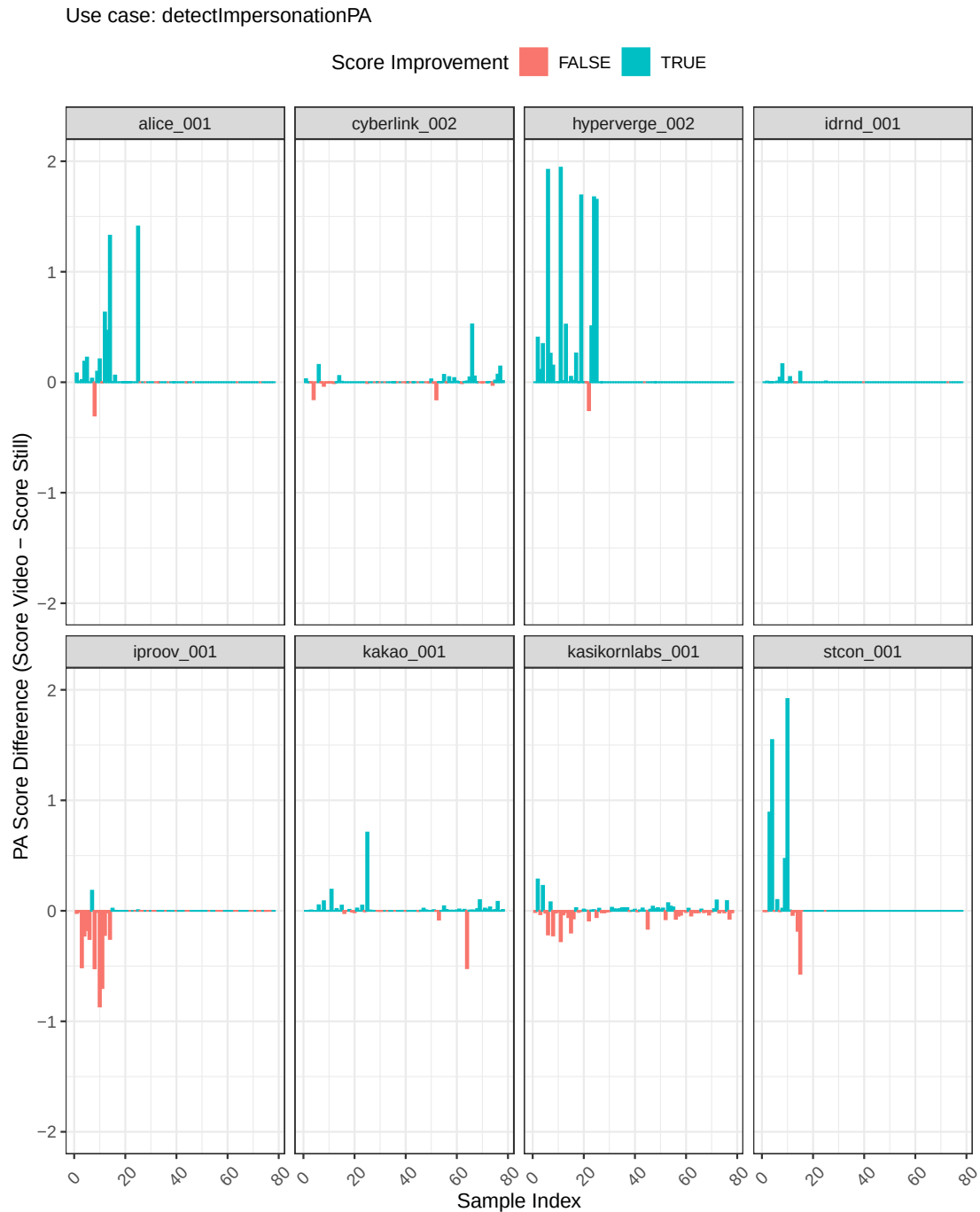


Fig. 5. This plot presents 1) pairwise PA PAD score differences between still and video scores of the same collection event and 2) whether or not a video sequence of the same collection event yields improvements over a single still image for better PA prediction outcomes. Teal colored lines represent improvement in PA PAD scores when a video is provided as input (vs. a still image), and the length of the line represents the magnitude of improvement (longer lines mean more improvement). Red lines indicate degradation of PA PAD scores with video input (vs. still), which means PA prediction degrades when the input is a video when compared to a still image.

Use case: detectImpersonationPA

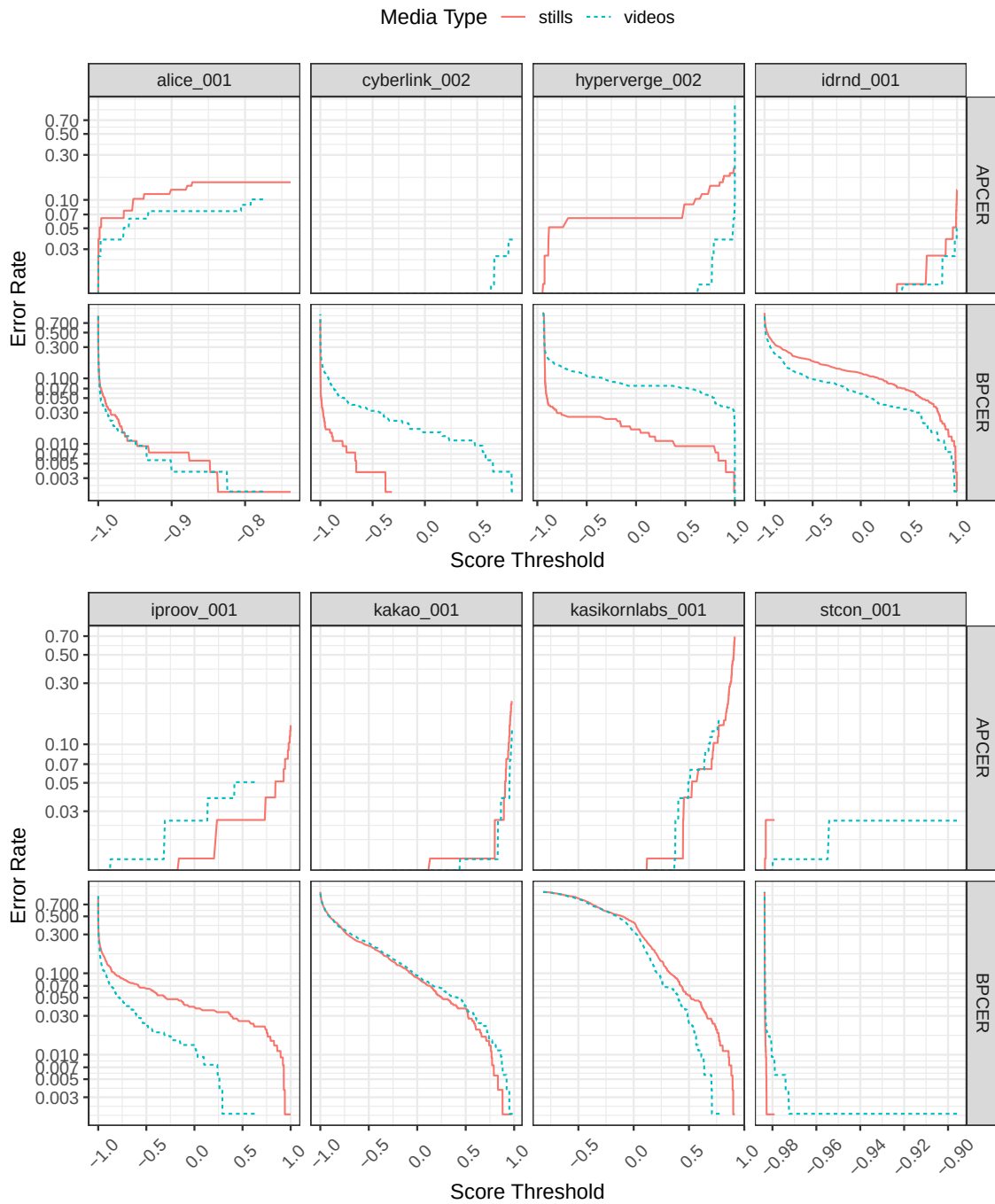


Fig. 6. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

5.3.2. Evasion

There were a total of 538 bona fide videos and corresponding stills and 209 evasion PA videos and corresponding stills across 5 different PA types. DET analysis was conducted using all 209 PA imagery collections and 538 bona fide imagery collections. Table 25 tabulates performance results by still vs. video imagery. Individual PAD performance with videos for each PA type is available in Appendix A.3.

Table 25. Use Case: detectEvasionPA - Stills vs. Videos

Algorithm	(Convenience) APCER @ BPCER=0.01		Algorithm	(Security) BPCER @ APCER=0.01	
	Stills	Videos		Stills	Videos
kakao-001	0.11	0.04	kakao-001	0.11	0.03
kakao-000	0.25	0.19	kakao-000	0.16	0.17
kasikornlabs-000	0.38	0.32	cyberlink-002	0.24	0.28
kasikornlabs-001	0.47	0.36	uxlabs-001	0.48	0.51
onfido-000	0.36	0.38	aware-001	0.49	0.57
neurotechnology-000	0.37	0.44	neurotechnology-000	1.00	0.57
onfido-001	0.53	0.49	alice-000	0.49	0.62
cyberlink-002	0.75	0.52	onfido-001	0.77	0.71
facedirect-002	0.83	0.72	aware-002	0.51	0.72
aware-002	0.68	0.81	onfido-000	0.74	0.81

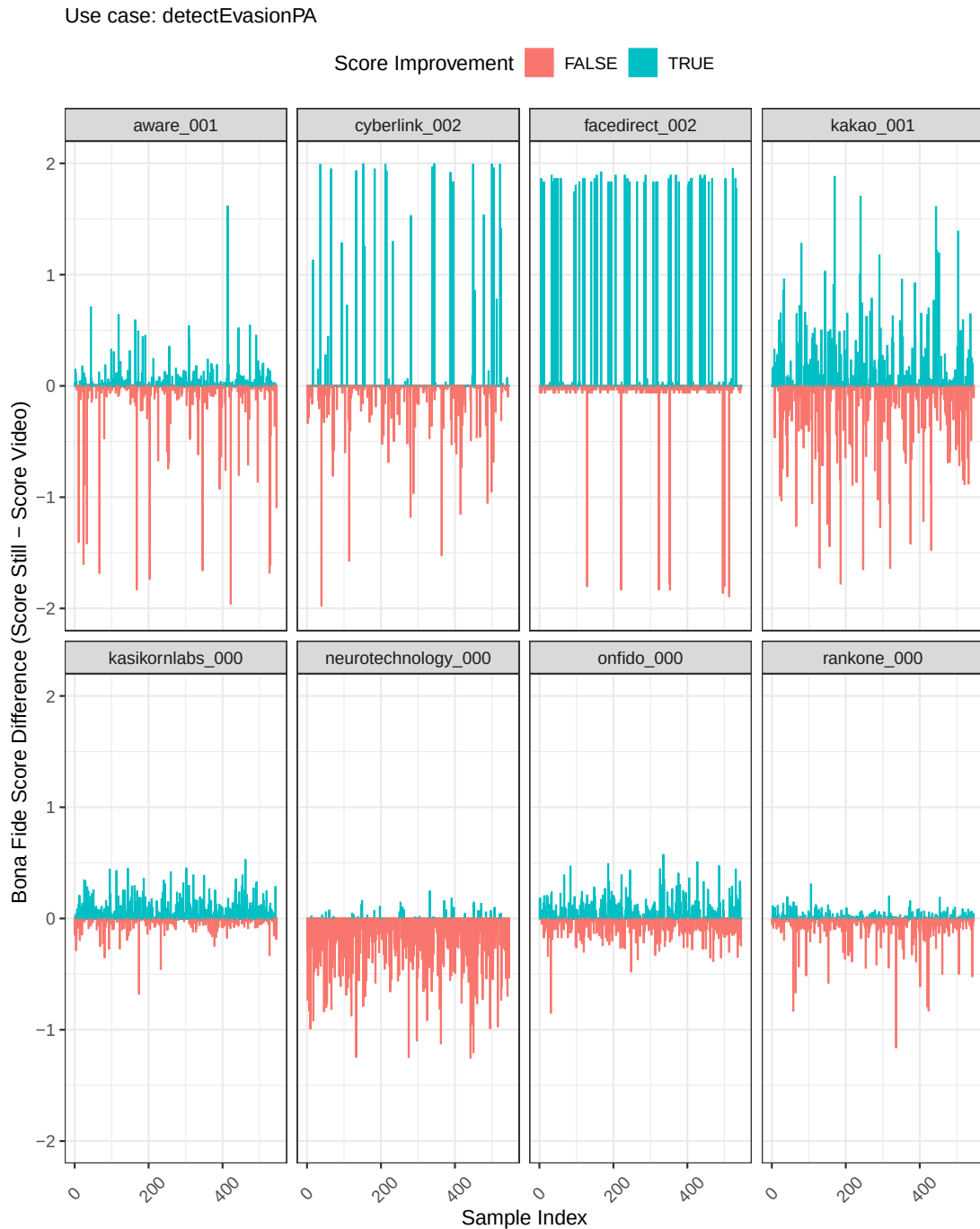


Fig. 7. This plot presents 1) pairwise bona fide PAD score differences between still and video scores of the same collection event and 2) whether or not a video sequence of the same collection event yields improvements over a single still image for better bona fide prediction outcomes. Teal colored lines represent improvement in bona fide PAD scores when a video is provided as input (vs. a still image), and the length of the line represents the magnitude of improvement (longer lines mean more improvement). Red lines indicate degradation of bona fide PAD scores with video input (vs. still), which means bona fide prediction degrades when the input is a video when compared to a still image.

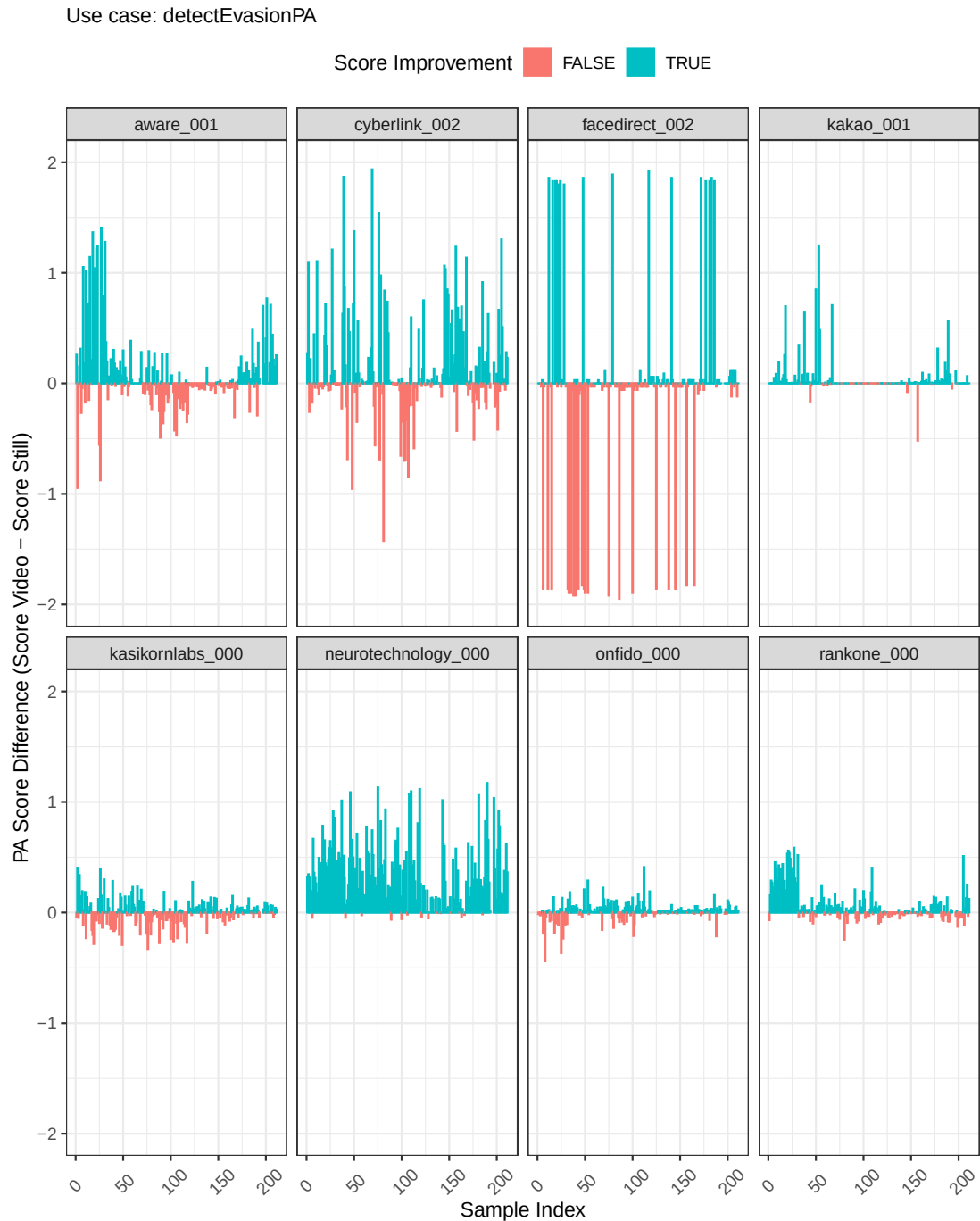


Fig. 8. This plot presents 1) pairwise PA PAD score differences between still and video scores of the same collection event and 2) whether or not a video sequence of the same collection event yields improvements over a single still image for better PA prediction outcomes. Teal colored lines represent improvement in PA PAD scores when a video is provided as input (vs. a still image), and the length of the line represents the magnitude of improvement (longer lines mean more improvement). Red lines indicate degradation of PA PAD scores with video input (vs. still), which means PA prediction degrades when the input is a video when compared to a still image.

Use case: detectEvasionPA

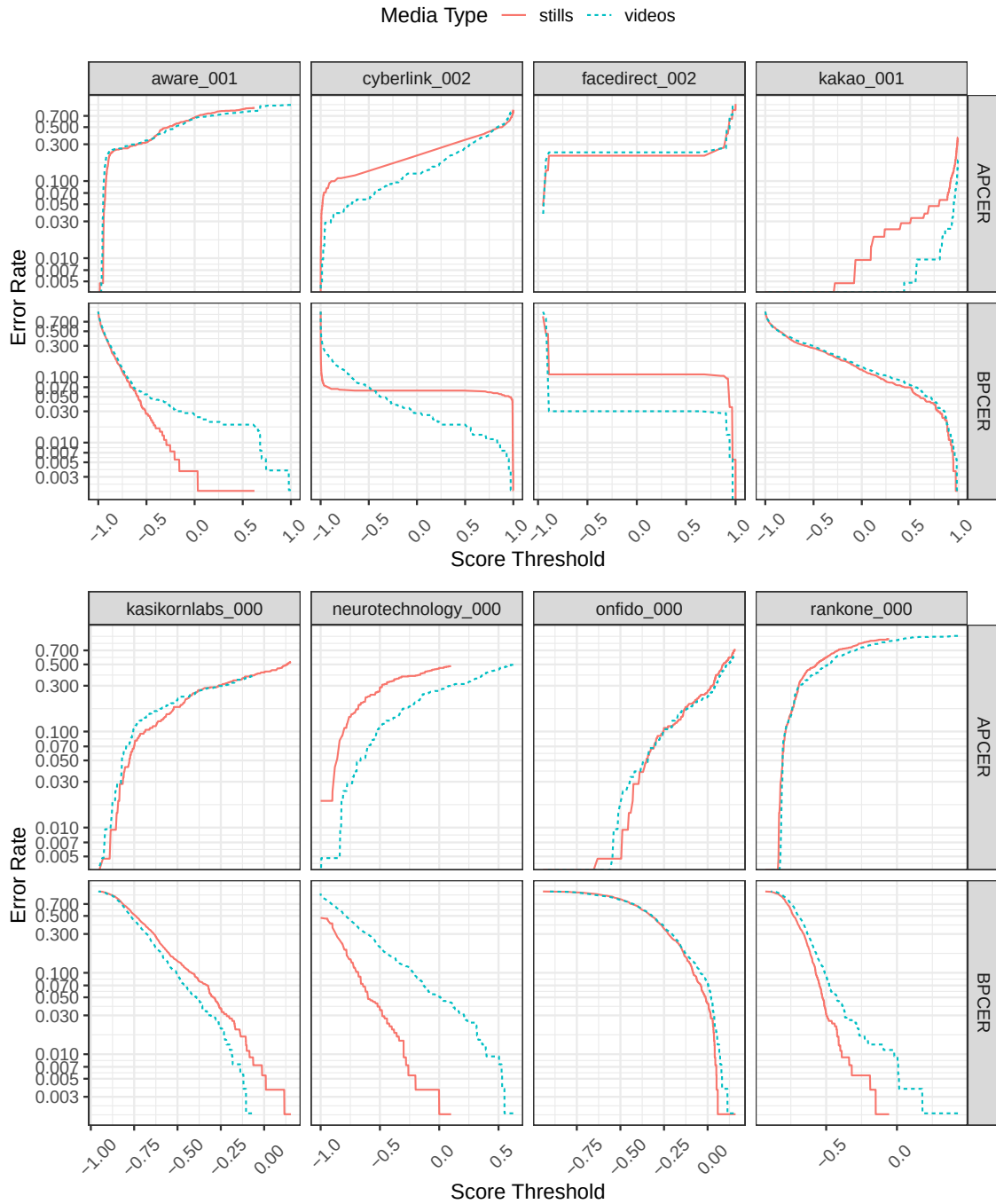


Fig. 9. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

5.4. Fusion

Biometric systems utilize the concept of fusion to combine information from multiple sources to try and improve recognition accuracy. Here, we investigate whether and to what extent fusion of multiple PAD algorithms might improve detection outcomes. While there is a plethora of fusion schemes that exist, as a proof of concept, we perform fusion across multiple PAD algorithms by simply fusing the scores using the sum rule. That is, given N algorithms, $\text{score}_{\text{fused}} = \sum_{alg=1}^N \text{score}_{alg}$. Tables 26 and 27 summarize the results of fusion for each detection task and PA type, with the fused performance ranking relative to all algorithms tested. For each use case, the algorithms selected for fusion were broadly top performing algorithms in one or more PA categories.

5.4.1. Impersonation

The results in Table 26 were generated by fusing four algorithms: cyberlink-002, idrnd-001, kakao-001, and stcon-001.

Table 26. Fusion Results - Use Case: detectImpersonationPA - Media Type: stills

PA Description	(Convenience)	Rank	(Security)	Rank
	APCER @ BPCER=0.01		BPCER @ APCER=0.01	
PA Type 1	0.004 ± 0.004	1	0.004	1
PA Type 3	0 ± 0	1	0.000	1
PA Type 4	0.1 ± 0.02	1	0.159	1
PA Type 7	0.006 ± 0.002	1	0.005	1
PA Type 8	0 ± 0	1	0.000	1
PA Type 8 (zoomed)	0 ± 0	1	0.003	1

5.4.2. Evasion

The results in Table 27 were generated by fusing four algorithms: aware-001, cyberlink-002, kakao-001, and onfido-000.

Table 27. Fusion Results - Use Case: detectEvasionPA - Media Type: stills

PA Description	(Convenience)	Rank	(Security)	Rank
	APCER @ BPCER=0.01		BPCER @ APCER=0.01	
PA Type 1	0.062 ± 0.008	1	0.088	1
PA Type 2	0.01 ± 0.01	1	0.009	1
PA Type 3	0.01 ± 0.01	1	0.006	1
PA Type 4	0.26 ± 0.03	1	0.193	2

PA Type 5	0.04 ± 0.03	3	0.023	2
PA Type 6	0 ± 0	1	0.000	3
PA Type 7	0.017 ± 0.004	1	0.023	1
PA Type 8	0.001 ± 0.001	1	0.006	1
PA Type 8 (zoomed)	0.15 ± 0.02	6	0.080	2
PA Type 9	0.003 ± 0.001	1	0.004	1

5.5. Demographic Effects

While demographic effects was not a primary evaluation objective, first-order analysis of results broken out by demographic groups may nevertheless be useful to developers. Initially, we assess BPCER/false detection rates across the different demographic groups represented in the test data. Tables 10 and 11 plot BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White-Male. While there is imbalance in the number of photos in each group, the error rate stands as the best estimate of false detection predictions for each group. While the BPCER for the smallest group may yield higher levels of uncertainty, we expect the level of uncertainty to remain small given the number of images processed.

Table 28. Demographic Data Summary, Bona Fide Stills

Demographic	Count
White-Male	5866
White-Female	9265
Black-Male	1119
Black-Female	2464
Asian-Male	665
Asian-Female	735

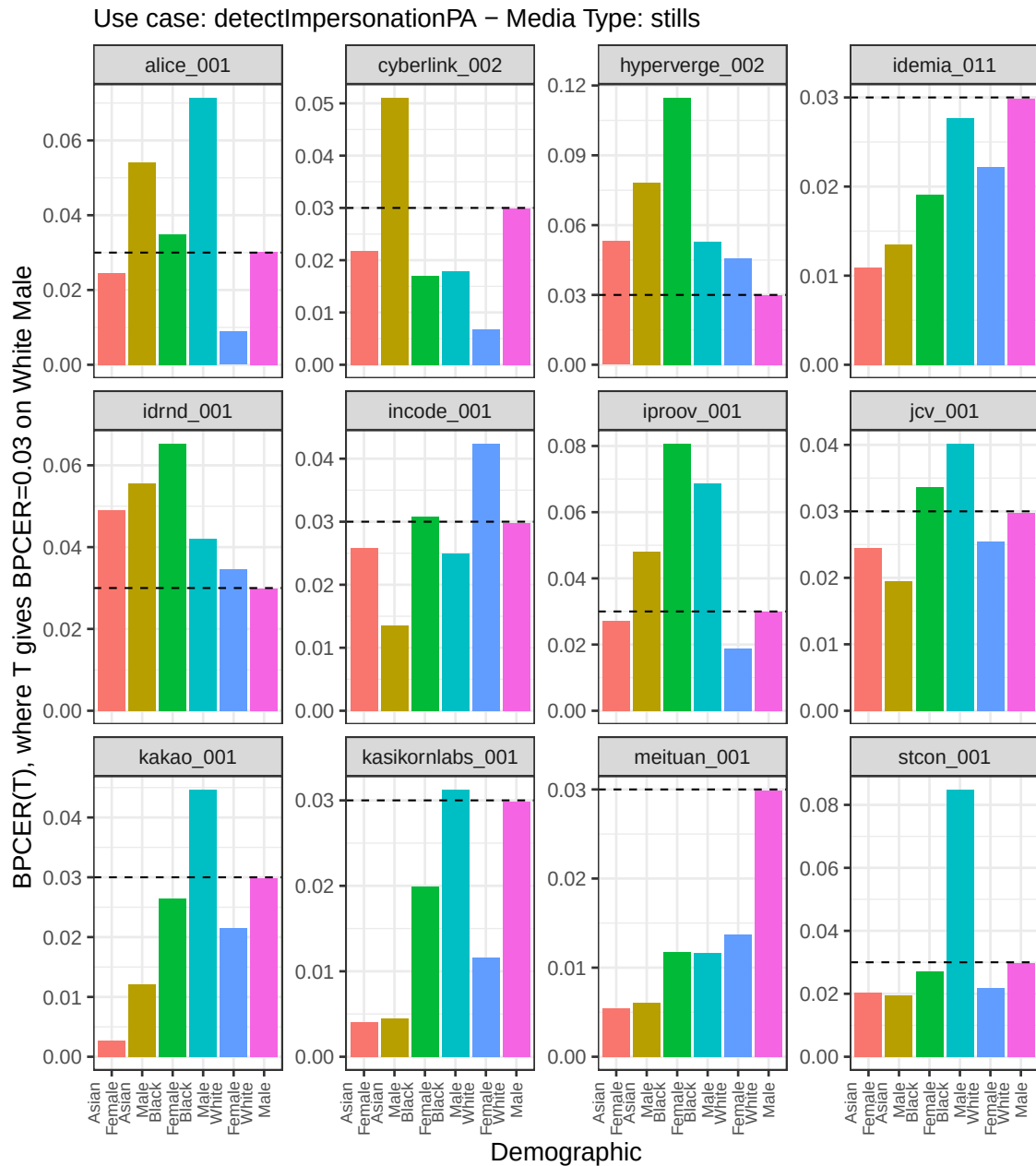


Fig. 10. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male.

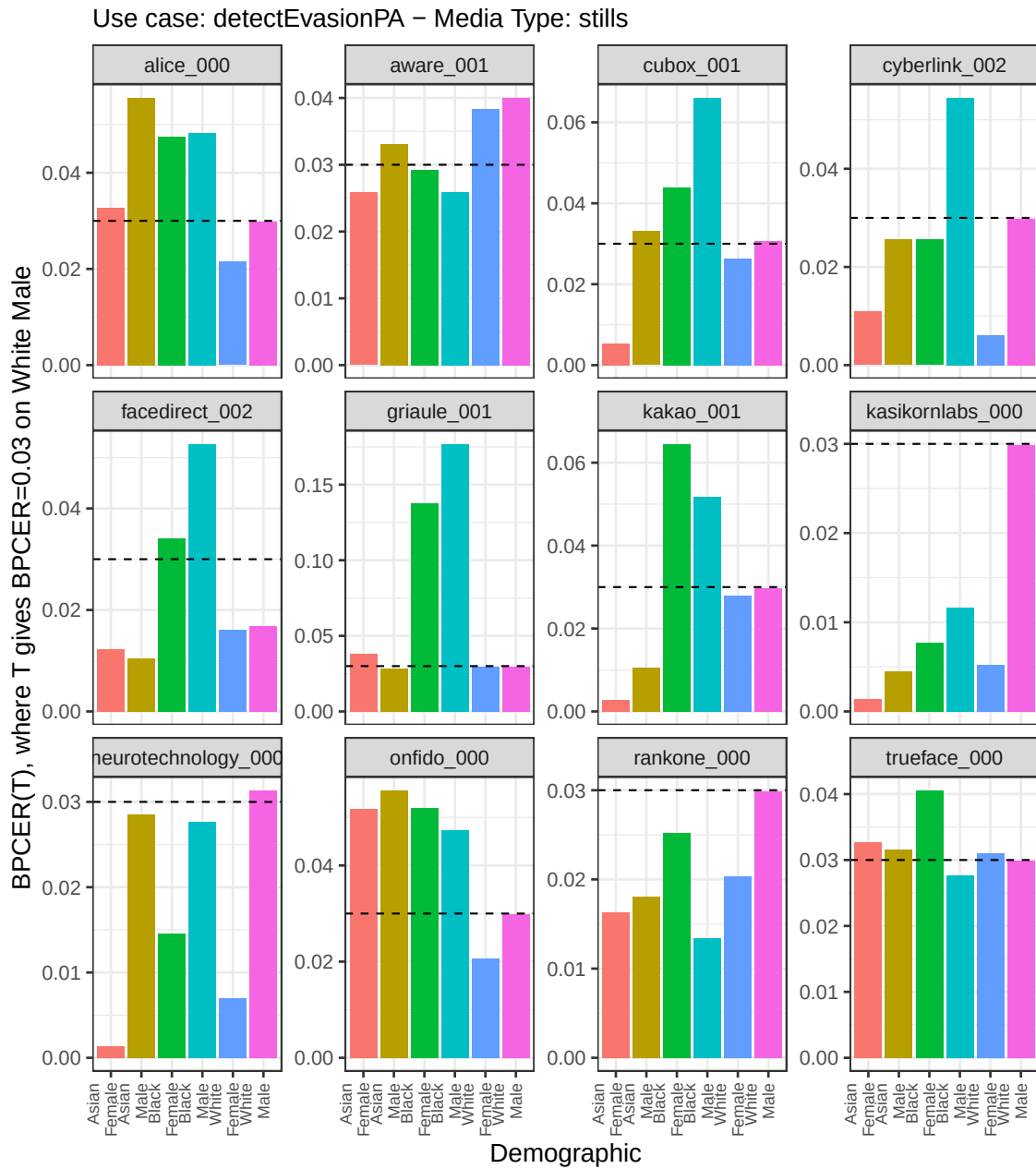


Fig. 11. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male.

References

- [1] JTC1/SC37 (2023) International Organization for Standardization: Information Technology – Biometric presentation attack detection – Part 1: Framework. *ISO/IEC 30107-1*, Vol. 2, pp 1–11. <https://www.iso.org/standard/83828.html>.
- [2] JTC1/SC37 (2023) International Organization for Standardization: Information Technology – Biometric presentation attack detection – Part 3: Testing and reporting. *ISO/IEC 30107-3*, Vol. 2, pp 1–39. <https://www.iso.org/standard/79520.html>.
- [3] Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial “gummy” fingers on fingerprint systems. *Optical Security and Counterfeit Deterrence Techniques IV*, ed van Renesse RL, *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, Vol. 4677, pp 275–289. <https://doi.org/10.1117/12.462719>
- [4] Sobell MG (2015) *A practical guide to Ubuntu Linux* (Pearson Education), 4th Ed. https://www.cl72.org/130gnuOS/sobell_ubuntu-linux.pdf.
- [5] Berg EJ (1936) *Heaviside’s operational calculus as applied to engineering and physics*. Electrical engineering texts (McGraw-Hill book company, inc.), 2nd Ed. Available at <https://books.google.com/books?id=jZw8AAAAIAAJ>.
- [6] Ngan M, Grother P, Hanaoka K, Hom A, Yang J (2023) PAD Concept, Evaluation Plan, and API. https://pages.nist.gov/frvt/api/FRVT_pad_api.pdf.

Appendix A. Detailed Algorithm Results

Appendix A.1. Timing

Table 29. Timing Statistics. This table includes the median duration (in microseconds) for each of the PAD function calls implemented in the algorithm submission. Timing was conducted over 1000 invocations of each function with a single input image of 1280×960 pixels. We measure the duration of all function calls using the C++ `std::chrono::high` resolution clock on an unloaded server-class machine.

Algorithm	detectImpersonationPA	detectEvasionPA
alchera_000	626762	426061
alice_000	567992	569786
alice_001	1914308	NOT IMPLEMENTED
aware_001	574519	1108573
aware_002	489973	646029
biocube_001	406687	NOT IMPLEMENTED
biocube_002	373057	NOT IMPLEMENTED
cubox_000	240890	241108
cubox_001	170798	171028
cyberlink_001	1356072	533984
cyberlink_002	3310836	3260528
facedirect_001	2577671	2575817
facedirect_002	3551555	3545257
facephi_000	1623628	NOT IMPLEMENTED
facephi_001	1608413	NOT IMPLEMENTED
griaule_000	233144	178602
griaule_001	207018	178152
hyperverge_001	828545	NOT IMPLEMENTED
hyperverge_002	1336211	NOT IMPLEMENTED
id3_001	54276	NOT IMPLEMENTED
idemia_010	1437127	NOT IMPLEMENTED
idemia_011	1548429	NOT IMPLEMENTED
idrnd_000	1071149	NOT IMPLEMENTED
idrnd_001	2211383	NOT IMPLEMENTED
idvisioncenter_001	1209794	NOT IMPLEMENTED
idvisioncenter_002	1158366	NOT IMPLEMENTED
iidentifi_000	454321	NOT IMPLEMENTED
incode_000	409352	NOT IMPLEMENTED
incode_001	168563	NOT IMPLEMENTED
innovatrics_001	161316	NOT IMPLEMENTED
innovatrics_002	82371	NOT IMPLEMENTED
intema_000	240864	NOT IMPLEMENTED
intema_001	438294	NOT IMPLEMENTED
iproov_000	481197	NOT IMPLEMENTED
iproov_001	478453	NOT IMPLEMENTED
jcv_001	1960542	1
jcv_002	1935989	NOT IMPLEMENTED

Table 29. Timing Statistics. This table includes the median duration (in microseconds) for each of the PAD function calls implemented in the algorithm submission. Timing was conducted over 1000 invocations of each function with a single input image of 1280x960 pixels. We measure the duration of all function calls using the C++ `std::chrono::high_resolution_clock` on an unloaded server-class machine. (*continued*)

Algorithm	detectImpersonationPA	detectEvasionPA
kakao_000	305931	307309
kakao_001	1994309	2000002
kasikornlabs_000	203020	203208
kasikornlabs_001	198511	196694
mbsolutions_000	165928	NOT IMPLEMENTED
mbsolutions_001	344484	NOT IMPLEMENTED
meituan_000	1679511	NOT IMPLEMENTED
meituan_001	1210108	NOT IMPLEMENTED
mobbl_000	167501	NOT IMPLEMENTED
mobbl_001	26255	NOT IMPLEMENTED
neurotechnology_000	767681	768336
neurotechnology_001	523325	522281
nsensekorea_000	52092	NOT IMPLEMENTED
nsensekorea_001	54822	NOT IMPLEMENTED
onfido_000	317243	319279
onfido_001	318573	318255
papago_001	426208	425695
pxl_000	66307	NOT IMPLEMENTED
pxl_001	64185	NOT IMPLEMENTED
rankone_000	417360	219247
rankone_001	412683	217497
saffe_001	17277	NOT IMPLEMENTED
saffe_002	26799	NOT IMPLEMENTED
spooff_000	158543	384100
stcon_000	1877903	NOT IMPLEMENTED
stcon_001	3692479	NOT IMPLEMENTED
tech5_001	142069	NOT IMPLEMENTED
techsign_000	565129	NOT IMPLEMENTED
techsign_001	869578	NOT IMPLEMENTED
trueface_000	250897	1732879
uxlabs_001	201687	201675
veridas_001	613979	NOT IMPLEMENTED
veridas_002	1912806	NOT IMPLEMENTED
verigram_000	380375	NOT IMPLEMENTED
verigram_001	828047	NOT IMPLEMENTED
verihubs-inteligensia_000	74964	NOT IMPLEMENTED
verihubs-inteligensia_001	89524	NOT IMPLEMENTED
vida_001	87030	NOT IMPLEMENTED
vida_002	106467	NOT IMPLEMENTED
visteam_001	85377	NOT IMPLEMENTED
visteam_002	68138	NOT IMPLEMENTED
yoontik_001	765220	NOT IMPLEMENTED

Table 29. Timing Statistics. This table includes the median duration (in microseconds) for each of the PAD function calls implemented in the algorithm submission. Timing was conducted over 1000 invocations of each function with a single input image of 1280x960 pixels. We measure the duration of all function calls using the C++ `std::chrono::high` resolution clock on an unloaded server-class machine. (*continued*)

Algorithm	detectImpersonationPA	detectEvasionPA
yoonik_002	926897	NOT IMPLEMENTED
yoti_001	10590583	NOT IMPLEMENTED
yoti_002	10605311	NOT IMPLEMENTED

Appendix A.2. Impersonation

Table 30. PA Type 1 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
kakao-001	0.000	0.000	0.07 ± 0.01	1	0.105	3
idrnd-001	0.000	0.000	0.1 ± 0.02	2	0.082	2
idrnd-000	0.000	0.000	0.12 ± 0.02	3	0.133	4
stcon-001	0.000	0.000	0.13 ± 0.02	4	0.346	7
iproov-001	0.000	0.000	0.16 ± 0.02	5	0.377	10
cyberlink-002	0.000	0.000	0.18 ± 0.02	6	0.207	5
kakao-000	0.000	0.000	0.31 ± 0.03	7	0.719	27
stcon-000	0.000	0.000	0.31 ± 0.03	8	0.482	13
cyberlink-001	0.000	0.000	0.42 ± 0.03	9	0.382	11
onfido-000	0.001	0.000	0.47 ± 0.03	10	0.825	37
kasikornlabs-000	0.000	0.000	0.52 ± 0.03	11	0.348	8
alice-001	0.000	0.000	0.52 ± 0.03	12	1.000	67
veridas-002	0.000	0.000	0.53 ± 0.03	13	0.524	14
iidentifii-000	0.000	0.000	0.57 ± 0.03	14	0.753	31
idemia-011	0.000	0.000	0.6 ± 0.03	15	0.779	34
kasikornlabs-001	0.000	0.000	0.6 ± 0.03	16	0.437	12
hyperverge-002	0.000	0.000	0.63 ± 0.03	17	0.989	55
aware-002	0.000	0.000	0.64 ± 0.03	18	0.356	9
veridas-001	0.000	0.000	0.64 ± 0.03	19	0.555	16
incode-001	0.000	0.000	0.64 ± 0.03	20	1.000	67
onfido-001	0.001	0.000	0.65 ± 0.03	21	0.720	28
hyperverge-001	0.000	0.000	0.67 ± 0.03	22	1.000	67
intema-001	0.000	0.000	0.72 ± 0.03	23	0.574	19
meituan-001	0.000	0.000	0.73 ± 0.03	24	1.000	67
neurotechnology-000	0.000	0.000	0.74 ± 0.03	25	1.000	67
innovatrics-002	0.000	0.000	0.76 ± 0.03	26	0.744	30
intema-000	0.000	0.000	0.79 ± 0.02	27	0.635	23
rankone-000	0.000	0.000	0.79 ± 0.02	28	0.728	29
verihubs-inteligensia-001	0.000	0.000	0.8 ± 0.02	29	0.712	26
verihubs-inteligensia-000	0.000	0.000	0.81 ± 0.02	30	0.893	40
visteam-002	0.000	0.000	0.84 ± 0.02	31	1.000	67
facedirect-002	0.000	0.000	0.84 ± 0.02	32	1.000	67
innovatrics-001	0.000	0.000	0.85 ± 0.02	33	0.688	25
vida-002	0.000	0.000	0.85 ± 0.02	34	0.978	52
mbsolutions-001	0.069	0.007	0.85 ± 0.02	35	1.000	67
saffe-002	0.001	0.000	0.86 ± 0.02	36	0.913	41
idemia-010	0.002	0.000	0.86 ± 0.02	37	0.580	20
facedirect-001	0.000	0.000	0.88 ± 0.02	38	0.967	50
incode-000	0.000	0.000	0.89 ± 0.02	39	0.536	15

Table 30. PA Type 1 - Use Case: detectImpersonationPA - Media Type: stills (*continued*)

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
saffe-001	0.001	0.000	0.9 ± 0.02	40	0.956	47
meituan-000	0.000	0.000	0.9 ± 0.02	41	0.989	55
vida-001	0.000	0.000	0.9 ± 0.02	42	0.966	49
jcv-001	0.002	0.000	0.92 ± 0.02	43	1.000	67
rankone-001	0.000	0.000	0.92 ± 0.02	44	0.762	32
idvisioncenter-001	0.000	0.000	0.92 ± 0.02	45	0.988	54
jcv-002	0.002	0.000	0.93 ± 0.02	46	1.000	67
griaule-001	0.000	0.000	0.94 ± 0.01	47	1.000	67
mbsolutions-000	0.000	0.000	0.94 ± 0.01	48	1.000	67
pxl-001	0.001	0.000	0.94 ± 0.01	49	0.929	42
idvisioncenter-002	0.000	0.000	0.95 ± 0.01	50	0.967	50
visteam-001	0.000	0.000	0.96 ± 0.01	51	0.998	58
verigram-001	0.000	0.000	0.96 ± 0.01	52	0.863	38
techsign-001	0.007	0.007	0.96 ± 0.01	53	1.000	67
biocube-001	0.000	0.000	0.96 ± 0.01	54	0.961	48
techsign-000	0.000	0.000	0.96 ± 0.01	55	1.000	59
ymoonik-002	0.000	0.000	0.96 ± 0.01	56	0.945	45
nsensekorea-001	0.000	0.000	0.97 ± 0.01	57	1.000	59
biocube-002	0.000	0.000	0.97 ± 0.01	58	1.000	67
nsensekorea-000	0.000	0.000	0.97 ± 0.01	58	1.000	59
id3-001	0.000	0.000	0.973 ± 0.009	60	0.871	39
cubox-000	0.000	0.000	0.979 ± 0.008	61	1.000	59
mobbl-000	0.000	0.000	0.984 ± 0.008	62	0.978	52
verigram-000	0.000	0.000	0.985 ± 0.007	63	0.934	43
spooff-000	0.000	0.000	0.986 ± 0.007	64	0.952	46
cubox-001	0.000	0.000	0.987 ± 0.007	65	1.000	59
papago-001	0.000	0.000	0.987 ± 0.007	66	1.000	59
mobbl-001	0.000	0.000	0.996 ± 0.004	67	0.989	55
tech5-001	0.001	0.002	0.996 ± 0.004	67	1.000	67
alchera-000	0.000	0.000	0.999 ± 0.001	69	1.000	59
alice-000	0.000	0.000	1 ± 0	70	0.565	18
aware-001	0.151	0.035	1 ± 0	70	0.308	6
facephi-000	0.000	0.000	1 ± 0	70	0.773	33
facephi-001	0.000	0.000	1 ± 0	70	0.687	24
griaule-000	0.000	0.000	1 ± 0	70	1.000	67
iproov-000	0.102	0.016	1 ± 0	70	0.069	1
neurotechnology-001	0.000	0.000	1 ± 0	70	0.813	36
pxl-000	0.001	0.000	1 ± 0	70	1.000	59
trueface-000	0.296	0.271	1 ± 0	70	0.810	35
uxlabs-001	0.000	0.000	1 ± 0	70	0.560	17
ymoonik-001	0.000	0.000	1 ± 0	70	0.934	43

Table 30. PA Type 1 - Use Case: detectImpersonationPA - Media Type: stills (*continued*)

Algorithm	APNRR	BPNRR	(Convenience)		(Security)	
			APCER @ BPCER=0.01	Rank	BPCER @ APCER=0.01	Rank
yoti-001	0.467	0.388	1 ± 0	70	0.628	21
yoti-002	0.463	0.393	1 ± 0	70	0.628	21

Table 31. PA Type 3 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
stcon-001	0.000	0.000	0 ± 0	1	0.000	1
stcon-000	0.000	0.000	0.005 ± 0.007	2	0.006	3
alice-001	0.000	0.000	0.01 ± 0.01	3	0.004	2
cyberlink-002	0.000	0.000	0.01 ± 0.01	3	0.007	4
idrnd-001	0.000	0.000	0.02 ± 0.02	5	0.012	5
incod-001	0.000	0.000	0.02 ± 0.02	5	0.070	15
idrnd-000	0.000	0.000	0.03 ± 0.02	7	0.027	9
cyberlink-001	0.000	0.000	0.03 ± 0.02	8	0.020	7
onfido-000	0.000	0.000	0.05 ± 0.03	9	0.036	10
iidentifi-000	0.000	0.000	0.06 ± 0.03	10	0.062	14
iproov-001	0.000	0.000	0.07 ± 0.04	11	0.248	25
onfido-001	0.000	0.000	0.09 ± 0.04	12	0.051	12
aware-002	0.000	0.000	0.1 ± 0.04	13	0.056	13
innovatrics-002	0.000	0.000	0.11 ± 0.05	14	0.098	17
facedirect-002	0.000	0.000	0.16 ± 0.05	15	0.989	66
veridas-002	0.000	0.000	0.25 ± 0.06	16	0.260	27
neurotechnology-000	0.000	0.000	0.26 ± 0.06	17	0.197	23
kasikornlabs-000	0.000	0.000	0.26 ± 0.06	18	0.251	26
kasikornlabs-001	0.000	0.000	0.29 ± 0.06	19	0.329	30
innovatrics-001	0.000	0.000	0.32 ± 0.06	20	0.352	31
idemia-011	0.000	0.000	0.35 ± 0.06	21	0.161	20
intema-001	0.000	0.000	0.39 ± 0.07	22	0.181	21
intema-000	0.000	0.000	0.42 ± 0.07	23	0.352	32
kakao-001	0.000	0.000	0.49 ± 0.07	24	0.365	33
incod-000	0.000	0.000	0.52 ± 0.07	25	0.085	16
meituan-001	0.000	0.000	0.54 ± 0.07	26	1.000	74
rankone-000	0.000	0.000	0.56 ± 0.07	27	0.423	34
meituan-000	0.000	0.000	0.6 ± 0.07	28	0.934	51
veridas-001	0.000	0.000	0.61 ± 0.07	29	0.284	28
jcv-001	0.000	0.000	0.62 ± 0.07	30	1.000	74
jcv-002	0.000	0.000	0.62 ± 0.07	30	1.000	74
idemia-010	0.000	0.000	0.65 ± 0.07	32	0.240	24
kakao-000	0.000	0.000	0.67 ± 0.06	33	0.824	45
vida-002	0.000	0.000	0.7 ± 0.06	34	0.643	41
visteam-002	0.000	0.000	0.71 ± 0.06	35	0.184	22
hyperverge-001	0.000	0.000	0.72 ± 0.06	36	1.000	74
hyperverge-002	0.000	0.000	0.72 ± 0.06	36	1.000	69
idvisioncenter-001	0.000	0.000	0.77 ± 0.06	38	0.976	62
facedirect-001	0.000	0.000	0.77 ± 0.06	39	0.536	37
mbsolutions-001	0.039	0.007	0.79 ± 0.06	40	1.000	74
saffe-002	0.000	0.000	0.82 ± 0.05	41	0.873	48

Table 31. PA Type 3 - Use Case: detectImpersonationPA - Media Type: stills (*continued*)

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
vida-001	0.000	0.000	0.83 ± 0.05	42	0.825	46
verihubs-inteligensia-001	0.000	0.000	0.86 ± 0.05	43	0.967	57
saffe-001	0.000	0.000	0.88 ± 0.04	44	0.883	49
rankone-001	0.000	0.000	0.88 ± 0.04	45	0.512	36
techsign-001	0.010	0.007	0.9 ± 0.04	46	0.699	43
verigram-001	0.000	0.000	0.91 ± 0.04	47	0.934	52
griaule-001	0.000	0.000	0.91 ± 0.04	48	1.000	74
cubox-000	0.000	0.000	0.92 ± 0.04	49	0.967	57
mobbl-001	0.000	0.000	0.94 ± 0.03	50	0.967	57
cubox-001	0.000	0.000	0.95 ± 0.03	51	0.934	53
visteam-001	0.000	0.000	0.95 ± 0.03	51	0.967	57
verihubs-inteligensia-000	0.000	0.000	0.95 ± 0.03	53	0.853	47
biocube-001	0.000	0.000	0.96 ± 0.03	54	0.995	68
biocube-002	0.000	0.000	0.96 ± 0.03	54	1.000	74
verigram-000	0.000	0.000	0.96 ± 0.03	56	0.945	56
yoonik-002	0.000	0.000	0.96 ± 0.03	56	0.945	55
pxl-001	0.000	0.000	0.97 ± 0.02	58	0.555	39
mbolutions-000	0.000	0.000	0.97 ± 0.02	59	1.000	74
spooff-000	0.000	0.000	0.97 ± 0.02	59	0.975	61
idvisioncenter-002	0.000	0.000	0.98 ± 0.02	61	0.762	44
nsensekorea-000	0.000	0.000	0.98 ± 0.02	61	1.000	69
nsensekorea-001	0.000	0.000	0.98 ± 0.02	61	1.000	69
id3-001	0.000	0.000	0.995 ± 0.007	64	0.944	54
papago-001	0.000	0.000	0.995 ± 0.007	64	0.989	63
tech5-001	0.005	0.002	0.995 ± 0.007	64	0.994	67
alchera-000	0.000	0.000	1 ± 0	67	1.000	69
alice-000	0.000	0.000	1 ± 0	67	0.014	6
aware-001	0.072	0.035	1 ± 0	67	0.045	11
facephi-000	0.000	0.000	1 ± 0	67	0.152	19
facephi-001	0.000	0.000	1 ± 0	67	0.124	18
griaule-000	0.000	0.000	1 ± 0	67	1.000	74
iproov-000	0.068	0.016	1 ± 0	67	0.021	8
mobbl-000	0.000	0.000	1 ± 0	67	0.989	63
neurotechnology-001	0.000	0.000	1 ± 0	67	0.294	29
pxl-000	0.000	0.000	1 ± 0	67	1.000	69
techsign-000	0.000	0.000	1 ± 0	67	0.989	63
trueface-000	0.261	0.271	1 ± 0	67	0.686	42
uxlabs-001	0.000	0.000	1 ± 0	67	0.447	35
yoonik-001	0.000	0.000	1 ± 0	67	0.913	50
yoti-001	0.473	0.388	1 ± 0	67	0.548	38
yoti-002	0.473	0.393	1 ± 0	67	0.580	40

Table 32. PA Type 4 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
cyberlink-002	0.000	0.000	0.13 ± 0.03	1	0.207	2
cyberlink-001	0.000	0.000	0.18 ± 0.03	2	0.408	7
stcon-001	0.000	0.000	0.19 ± 0.03	3	0.670	20
stcon-000	0.000	0.000	0.29 ± 0.04	4	0.771	26
idrnd-001	0.000	0.000	0.42 ± 0.04	5	0.395	5
idrnd-000	0.000	0.000	0.47 ± 0.04	6	0.395	5
meituan-001	0.000	0.000	0.53 ± 0.04	7	1.000	68
iproov-001	0.000	0.000	0.55 ± 0.04	8	0.613	13
alice-001	0.000	0.000	0.56 ± 0.04	9	1.000	68
jcv-001	0.000	0.000	0.59 ± 0.04	10	0.881	36
kasikornlabs-000	0.000	0.000	0.62 ± 0.04	11	0.452	9
kasikornlabs-001	0.000	0.000	0.62 ± 0.04	12	0.555	11
jcv-002	0.000	0.000	0.63 ± 0.04	13	1.000	68
vida-001	0.000	0.000	0.64 ± 0.04	14	0.447	8
meituan-000	0.000	0.000	0.66 ± 0.04	15	0.956	48
kakao-001	0.000	0.000	0.66 ± 0.04	16	0.649	17
intema-000	0.000	0.000	0.7 ± 0.04	17	0.628	16
intema-001	0.000	0.000	0.7 ± 0.04	18	0.463	10
idemia-011	0.000	0.000	0.71 ± 0.04	19	0.621	14
onfido-001	0.000	0.000	0.74 ± 0.03	20	0.621	15
veridas-002	0.000	0.000	0.75 ± 0.03	21	0.797	28
aware-002	0.000	0.000	0.76 ± 0.03	22	0.322	4
iidentifi-000	0.000	0.000	0.77 ± 0.03	23	0.704	23
vida-002	0.000	0.000	0.81 ± 0.03	24	0.934	42
onfido-000	0.000	0.000	0.82 ± 0.03	25	0.788	27
hyperverge-002	0.000	0.000	0.82 ± 0.03	26	1.000	62
verihubs-inteligensia-001	0.000	0.000	0.84 ± 0.03	27	0.893	37
incode-001	0.000	0.000	0.84 ± 0.03	28	1.000	68
hyperverge-001	0.000	0.000	0.84 ± 0.03	29	1.000	68
veridas-001	0.000	0.000	0.86 ± 0.03	30	0.762	25
innovatrics-002	0.000	0.000	0.88 ± 0.03	31	0.873	35
kakao-000	0.000	0.000	0.88 ± 0.03	32	0.931	40
incode-000	0.000	0.000	0.89 ± 0.03	33	0.806	29
facedirect-001	0.000	0.000	0.9 ± 0.02	34	0.989	57
idemia-010	0.000	0.000	0.9 ± 0.02	35	0.665	18
cubox-001	0.000	0.000	0.9 ± 0.02	36	0.967	52
innovatrics-001	0.000	0.000	0.91 ± 0.02	37	0.711	24
neurotechnology-000	0.000	0.000	0.91 ± 0.02	38	1.000	68
techsign-001	0.003	0.007	0.91 ± 0.02	39	1.000	68
visteam-002	0.000	0.000	0.92 ± 0.02	40	1.000	68
mbsolutions-001	0.050	0.007	0.92 ± 0.02	41	1.000	68

Table 32. PA Type 4 - Use Case: detectImpersonationPA - Media Type: stills (*continued*)

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
rankone-001	0.000	0.000	0.92 ± 0.02	42	0.834	31
saffe-002	0.000	0.000	0.92 ± 0.02	43	0.934	43
griaule-001	0.000	0.000	0.93 ± 0.02	44	1.000	68
mbsolutions-000	0.000	0.000	0.95 ± 0.02	45	1.000	68
cubox-000	0.000	0.000	0.95 ± 0.02	46	0.967	52
rankone-000	0.000	0.000	0.95 ± 0.02	46	0.924	38
verihubs-inteligensia-000	0.000	0.000	0.95 ± 0.02	46	0.989	57
verigram-001	0.000	0.000	0.96 ± 0.02	49	0.966	51
idvisioncenter-001	0.000	0.000	0.96 ± 0.01	50	0.934	41
saffe-001	0.000	0.000	0.96 ± 0.01	50	0.934	43
visteam-001	0.000	0.000	0.96 ± 0.02	50	0.967	52
tech5-001	0.000	0.002	0.98 ± 0.01	53	1.000	68
techsign-000	0.000	0.000	0.98 ± 0.01	53	0.945	47
facedirect-002	0.000	0.000	0.98 ± 0.01	55	0.989	61
pxl-001	0.000	0.000	0.98 ± 0.01	55	0.835	32
spooff-000	0.000	0.000	0.987 ± 0.009	57	0.960	49
idvisioncenter-002	0.000	0.000	0.99 ± 0.007	58	0.924	38
yoonik-002	0.000	0.000	0.99 ± 0.007	58	0.945	45
alchera-000	0.000	0.000	0.992 ± 0.007	60	1.000	62
id3-001	0.000	0.000	0.992 ± 0.007	60	0.861	34
mobbl-001	0.000	0.000	0.992 ± 0.007	60	0.989	57
papago-001	0.000	0.000	0.992 ± 0.007	60	0.989	57
biocube-001	0.000	0.000	0.994 ± 0.006	64	0.984	56
biocube-002	0.000	0.000	0.995 ± 0.006	65	1.000	68
nsensekorea-000	0.000	0.000	0.995 ± 0.006	65	1.000	62
nsensekorea-001	0.000	0.000	0.995 ± 0.006	65	1.000	62
mobbl-000	0.000	0.000	0.998 ± 0.002	68	0.978	55
alice-000	0.000	0.000	1 ± 0	69	0.813	30
aware-001	0.139	0.035	1 ± 0	69	0.200	1
facephi-000	0.000	0.000	1 ± 0	69	0.610	12
facephi-001	0.000	0.000	1 ± 0	69	0.677	22
griaule-000	0.000	0.000	1 ± 0	69	1.000	68
iproov-000	0.073	0.016	1 ± 0	69	0.315	3
neurotechnology-001	0.000	0.000	1 ± 0	69	0.853	33
pxl-000	0.000	0.000	1 ± 0	69	1.000	62
trueface-000	0.181	0.271	1 ± 0	69	1.000	68
uxlabs-001	0.000	0.000	1 ± 0	69	0.964	50
verigram-000	0.000	0.000	1 ± 0	69	1.000	62
yoonik-001	0.000	0.000	1 ± 0	69	0.945	45
yoti-001	0.380	0.388	1 ± 0	69	0.672	21
yoti-002	0.438	0.393	1 ± 0	69	0.665	18

Table 33. PA Type 7 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
cyberlink-002	0.000	0.000	0.012 ± 0.003	1	0.012	1
cyberlink-001	0.000	0.000	0.052 ± 0.006	2	0.095	2
kakao-001	0.000	0.000	0.06 ± 0.007	3	0.159	3
alice-001	0.000	0.000	0.108 ± 0.009	4	0.345	8
kakao-000	0.000	0.000	0.16 ± 0.01	5	0.703	31
hyperverge-002	0.000	0.000	0.31 ± 0.01	6	0.989	60
veridas-002	0.000	0.000	0.32 ± 0.01	7	0.291	6
onfido-001	0.000	0.000	0.33 ± 0.01	8	0.263	4
idrnd-000	0.000	0.000	0.33 ± 0.01	9	0.348	9
idrnd-001	0.000	0.000	0.42 ± 0.01	10	0.356	10
onfido-000	0.000	0.000	0.42 ± 0.01	11	0.696	30
hyperverge-001	0.000	0.000	0.47 ± 0.01	12	1.000	68
idemia-011	0.000	0.000	0.48 ± 0.01	13	0.643	28
vida-002	0.000	0.000	0.5 ± 0.01	14	0.594	25
veridas-001	0.000	0.000	0.5 ± 0.01	15	0.297	7
iproov-001	0.000	0.000	0.51 ± 0.01	16	0.489	17
rankone-000	0.000	0.000	0.56 ± 0.01	17	0.530	23
vida-001	0.000	0.000	0.62 ± 0.01	18	0.524	21
incode-001	0.000	0.000	0.62 ± 0.01	19	1.000	68
meituan-001	0.000	0.000	0.64 ± 0.01	20	1.000	68
stcon-000	0.000	0.000	0.64 ± 0.01	21	0.729	35
jcv-001	0.001	0.000	0.65 ± 0.01	22	1.000	68
neurotechnology-000	0.000	0.000	0.65 ± 0.01	23	0.525	22
meituan-000	0.000	0.000	0.69 ± 0.01	24	0.978	54
jcv-002	0.001	0.000	0.69 ± 0.01	25	1.000	68
innovatrics-002	0.000	0.000	0.71 ± 0.01	26	0.275	5
stcon-001	0.000	0.000	0.72 ± 0.01	27	0.747	36
incode-000	0.000	0.000	0.72 ± 0.01	28	0.696	29
verigram-001	0.000	0.000	0.74 ± 0.01	29	0.797	41
verihubs-inteligensia-001	0.000	0.000	0.77 ± 0.01	30	0.815	43
aware-002	0.000	0.000	0.8 ± 0.01	31	0.479	16
intema-000	0.000	0.000	0.81 ± 0.01	32	0.770	38
iidentifi-000	0.000	0.000	0.81 ± 0.01	33	0.873	45
intema-001	0.000	0.000	0.82 ± 0.01	34	0.561	24
kasikornlabs-000	0.000	0.000	0.84 ± 0.01	35	0.728	33
facedirect-001	0.000	0.000	0.84 ± 0.01	36	0.967	52
kasikornlabs-001	0.000	0.000	0.86 ± 0.01	37	0.753	37
facedirect-002	0.000	0.000	0.86 ± 0.01	38	1.000	68
verihubs-inteligensia-000	0.000	0.000	0.87 ± 0.01	39	0.844	44
techsign-001	0.006	0.007	0.884 ± 0.009	40	1.000	68
innovatrics-001	0.000	0.000	0.885 ± 0.009	41	0.711	32

Table 33. PA Type 7 - Use Case: detectImpersonationPA - Media Type: stills (*continued*)

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
griaule-001	0.000	0.000	0.887 ± 0.009	42	1.000	68
idemia-010	0.000	0.000	0.892 ± 0.009	43	0.454	15
mbsolutions-000	0.000	0.000	0.897 ± 0.009	44	1.000	68
saffe-002	0.000	0.000	0.901 ± 0.009	45	0.924	47
rankone-001	0.000	0.000	0.913 ± 0.008	46	0.728	33
mbsolutions-001	0.047	0.007	0.918 ± 0.008	47	1.000	68
saffe-001	0.000	0.000	0.922 ± 0.008	48	0.934	49
cubox-001	0.000	0.000	0.949 ± 0.006	49	0.945	50
yoonik-002	0.000	0.000	0.971 ± 0.005	50	0.806	42
nsensekorea-001	0.000	0.000	0.971 ± 0.005	51	1.000	63
nsensekorea-000	0.000	0.000	0.972 ± 0.005	52	1.000	63
techsign-000	0.000	0.000	0.972 ± 0.005	53	0.978	55
visteam-002	0.000	0.000	0.977 ± 0.004	54	1.000	68
visteam-001	0.000	0.000	0.98 ± 0.004	55	0.977	53
cubox-000	0.000	0.000	0.98 ± 0.004	56	0.989	60
verigram-000	0.000	0.000	0.984 ± 0.004	57	1.000	63
papago-001	0.000	0.000	0.987 ± 0.003	58	1.000	63
mobbl-001	0.000	0.000	0.988 ± 0.003	59	0.978	55
id3-001	0.000	0.000	0.99 ± 0.003	60	0.512	20
spooff-000	0.000	0.000	0.99 ± 0.003	61	0.988	59
pxl-001	0.000	0.000	0.992 ± 0.003	62	0.929	48
biocube-002	0.000	0.000	0.992 ± 0.003	63	1.000	68
idvisioncenter-001	0.000	0.000	0.994 ± 0.002	64	0.965	51
biocube-001	0.000	0.000	0.994 ± 0.002	65	0.984	58
idvisioncenter-002	0.000	0.000	0.995 ± 0.002	66	0.913	46
tech5-001	0.003	0.002	0.997 ± 0.002	67	1.000	68
mobbl-000	0.000	0.000	0.998 ± 0.001	68	0.978	55
alchera-000	0.000	0.000	1 ± 0.0005	69	1.000	63
alice-000	0.000	0.000	1 ± 0	70	0.381	12
aware-001	0.149	0.035	1 ± 0	70	0.495	18
facephi-000	0.000	0.000	1 ± 0	70	0.413	13
facephi-001	0.000	0.000	1 ± 0	70	0.442	14
griaule-000	0.000	0.000	1 ± 0	70	1.000	68
iproov-000	0.084	0.016	1 ± 0	70	0.377	11
neurotechnology-001	0.000	0.000	1 ± 0	70	0.773	39
pxl-000	0.000	0.000	1 ± 0	70	0.989	60
trueface-000	0.309	0.271	1 ± 0	70	1.000	68
uxlabs-001	0.000	0.000	1 ± 0	70	0.500	19
yoonik-001	0.000	0.000	1 ± 0	70	0.788	40
yoti-001	0.442	0.388	1 ± 0	70	0.628	27
yoti-002	0.502	0.393	1 ± 0	70	0.600	26

Table 34. PA Type 8 - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
alice-001	0.000	0.000	0 ± 0	1	0.000	2
idemia-011	0.000	0.000	0 ± 0	1	0.002	4
idrnd-000	0.000	0.000	0 ± 0	1	0.000	3
idrnd-001	0.000	0.000	0 ± 0	1	0.000	1
hyperverge-002	0.000	0.000	0.001 ± 0.001	5	0.003	6
kakao-001	0.000	0.000	0.001 ± 0.001	5	0.003	5
iproov-001	0.000	0.000	0.003 ± 0.002	7	0.005	8
meituan-001	0.000	0.000	0.004 ± 0.003	8	0.003	7
stcon-000	0.000	0.000	0.008 ± 0.005	9	0.007	10
hyperverge-001	0.000	0.000	0.008 ± 0.005	10	0.009	12
intema-001	0.000	0.000	0.008 ± 0.005	10	0.010	14
kakao-000	0.000	0.000	0.009 ± 0.005	12	0.005	9
innovatrics-001	0.000	0.000	0.01 ± 0.005	13	0.009	13
saffe-002	0.000	0.000	0.01 ± 0.005	13	0.008	11
jcv-001	0.004	0.000	0.012 ± 0.006	15	0.010	15
stcon-001	0.000	0.000	0.015 ± 0.006	16	0.019	21
cyberlink-002	0.000	0.000	0.016 ± 0.007	17	0.016	20
saffe-001	0.000	0.000	0.016 ± 0.006	17	0.024	26
onfido-001	0.000	0.000	0.017 ± 0.007	19	0.020	24
mbsolutions-001	0.075	0.007	0.018 ± 0.007	20	0.026	27
meituan-000	0.000	0.000	0.019 ± 0.007	21	0.099	37
jcv-002	0.004	0.000	0.021 ± 0.007	22	0.014	18
onfido-000	0.000	0.000	0.024 ± 0.008	23	0.019	21
intema-000	0.000	0.000	0.025 ± 0.008	24	0.045	30
incode-001	0.000	0.000	0.03 ± 0.01	25	0.021	25
cyberlink-001	0.000	0.000	0.04 ± 0.01	26	0.040	29
aware-002	0.000	0.000	0.08 ± 0.01	27	0.073	33
kasikornlabs-000	0.000	0.000	0.09 ± 0.02	28	0.126	39
verihubs-inteligensia-001	0.000	0.000	0.1 ± 0.02	29	0.070	32
neurotechnology-000	0.000	0.000	0.1 ± 0.02	30	0.095	36
mbsolutions-000	0.000	0.000	0.1 ± 0.02	31	0.229	46
verihubs-inteligensia-000	0.000	0.000	0.12 ± 0.02	32	0.115	38
vida-002	0.000	0.000	0.12 ± 0.02	33	0.062	31
kasikornlabs-001	0.000	0.000	0.15 ± 0.02	34	0.141	41
incode-000	0.000	0.000	0.19 ± 0.02	35	0.085	34
iidentifi-000	0.000	0.000	0.2 ± 0.02	36	0.151	43
idemia-010	0.000	0.000	0.22 ± 0.02	37	0.030	28
verigram-001	0.000	0.000	0.28 ± 0.02	38	0.141	41
rankone-000	0.000	0.000	0.34 ± 0.02	39	0.574	55
pxl-001	0.000	0.000	0.37 ± 0.02	40	0.408	50
rankone-001	0.000	0.000	0.39 ± 0.03	41	0.281	48

Table 34. PA Type 8 - Use Case: detectImpersonationPA - Media Type: stills (*continued*)

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
nsensekorea-001	0.000	0.000	0.41 ± 0.03	42	0.863	71
nsensekorea-000	0.000	0.000	0.41 ± 0.03	43	0.853	69
innovatrics-002	0.000	0.000	0.43 ± 0.03	44	0.501	53
veridas-001	0.000	0.000	0.45 ± 0.03	45	0.628	57
facedirect-002	0.000	0.000	0.47 ± 0.03	46	1.000	77
vida-001	0.000	0.000	0.48 ± 0.03	47	0.501	54
techsign-001	0.007	0.007	0.53 ± 0.03	48	0.669	58
idvisioncenter-001	0.000	0.000	0.6 ± 0.03	49	0.806	65
yoonek-002	0.000	0.000	0.6 ± 0.03	50	0.237	47
veridas-002	0.000	0.000	0.62 ± 0.03	51	0.903	74
mobbl-000	0.000	0.000	0.68 ± 0.02	52	0.745	62
visteam-002	0.000	0.000	0.71 ± 0.02	53	1.000	77
techsign-000	0.000	0.000	0.72 ± 0.02	54	0.587	56
verigram-000	0.000	0.000	0.72 ± 0.02	55	0.128	40
griaule-001	0.000	0.000	0.75 ± 0.02	56	1.000	77
idvisioncenter-002	0.000	0.000	0.79 ± 0.02	57	0.883	72
facedirect-001	0.000	0.000	0.86 ± 0.02	58	0.956	76
mobbl-001	0.000	0.000	0.86 ± 0.02	59	0.834	68
biocube-002	0.000	0.000	0.88 ± 0.02	60	0.834	67
cubox-001	0.000	0.000	0.88 ± 0.02	61	0.893	73
biocube-001	0.000	0.000	0.9 ± 0.02	62	0.779	63
cubox-000	0.000	0.000	0.9 ± 0.02	63	0.806	66
id3-001	0.000	0.000	0.92 ± 0.01	64	0.861	70
visteam-001	0.000	0.000	0.92 ± 0.01	65	0.934	75
spooff-000	0.000	0.000	0.96 ± 0.01	66	0.429	51
tech5-001	0.001	0.002	0.999 ± 0.001	67	1.000	77
alchera-000	0.000	0.000	1 ± 0	68	1.000	77
alice-000	0.000	0.000	1 ± 0	68	0.015	19
aware-001	0.114	0.035	1 ± 0	68	0.086	35
facephi-000	0.000	0.000	1 ± 0	68	0.011	16
facephi-001	0.000	0.000	1 ± 0	68	0.012	17
griaule-000	0.000	0.000	1 ± 0	68	0.468	52
iproov-000	0.103	0.016	1 ± 0	68	0.020	23
neurotechnology-001	0.000	0.000	1 ± 0	68	0.224	45
papago-001	0.000	0.000	1 ± 0	68	0.696	60
pxl-000	0.000	0.000	1 ± 0	68	1.000	77
trueface-000	0.308	0.271	1 ± 0	68	0.382	49
uxlabs-001	0.000	0.000	1 ± 0	68	0.678	59
yoonek-001	0.000	0.000	1 ± 0	68	0.193	44
yoti-001	0.462	0.388	1 ± 0	68	0.720	61
yoti-002	0.450	0.393	1 ± 0	68	0.788	64

Table 35. PA Type 8 (zoomed) - Use Case: detectImpersonationPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
idrnd-001	0.000	0.000	0.005 ± 0.004	1	0.006	1
idrnd-000	0.000	0.000	0.011 ± 0.005	2	0.010	2
stcon-000	0.000	0.000	0.018 ± 0.007	3	0.016	3
idemia-011	0.000	0.000	0.028 ± 0.009	4	0.026	5
kakao-001	0.000	0.000	0.031 ± 0.009	5	0.026	4
iproov-001	0.000	0.000	0.04 ± 0.01	6	0.047	10
jcv-001	0.007	0.000	0.05 ± 0.01	7	0.044	7
stcon-001	0.000	0.000	0.06 ± 0.01	8	0.091	13
onfido-001	0.003	0.000	0.06 ± 0.01	9	0.096	14
kakao-000	0.000	0.000	0.06 ± 0.01	10	0.089	12
onfido-000	0.003	0.000	0.07 ± 0.01	11	0.219	19
meituan-001	0.000	0.000	0.07 ± 0.01	12	0.045	8
jcv-002	0.007	0.000	0.07 ± 0.01	13	0.039	6
kasikornlabs-000	0.001	0.000	0.12 ± 0.02	14	0.574	44
saffe-002	0.000	0.000	0.12 ± 0.02	14	0.272	24
intema-000	0.000	0.000	0.14 ± 0.02	16	0.304	30
incode-001	0.000	0.000	0.14 ± 0.02	17	0.193	18
mbsolutions-001	0.079	0.007	0.15 ± 0.02	18	0.628	50
hyperverge-002	0.000	0.000	0.15 ± 0.02	19	0.989	73
saffe-001	0.000	0.000	0.17 ± 0.02	20	0.308	31
intema-001	0.000	0.000	0.17 ± 0.02	21	0.284	28
pxl-001	0.002	0.000	0.19 ± 0.02	22	0.275	27
alice-001	0.000	0.000	0.22 ± 0.02	23	1.000	74
kasikornlabs-001	0.001	0.000	0.22 ± 0.02	23	0.628	48
idemia-010	0.000	0.000	0.23 ± 0.02	25	0.130	15
vida-002	0.001	0.000	0.23 ± 0.02	26	0.628	48
hyperverge-001	0.000	0.000	0.23 ± 0.02	27	1.000	74
verihubs-inteligensia-000	0.000	0.000	0.26 ± 0.02	28	0.251	23
veridas-001	0.001	0.000	0.27 ± 0.02	29	0.484	37
verihubs-inteligensia-001	0.000	0.000	0.27 ± 0.02	30	0.272	24
iidentifi-000	0.000	0.000	0.28 ± 0.02	31	0.542	42
facedirect-002	0.000	0.000	0.3 ± 0.02	32	1.000	74
neurotechnology-000	0.000	0.000	0.3 ± 0.02	33	1.000	74
aware-002	0.000	0.000	0.31 ± 0.02	34	0.308	31
incode-000	0.000	0.000	0.31 ± 0.02	34	0.720	55
rankone-000	0.000	0.000	0.33 ± 0.02	36	0.561	43
meituan-000	0.000	0.000	0.34 ± 0.02	37	0.665	51
innovatrics-001	0.000	0.000	0.35 ± 0.02	38	0.245	21
rankone-001	0.000	0.000	0.37 ± 0.03	39	0.284	28
yoonek-002	0.000	0.000	0.37 ± 0.03	40	0.341	33
innovatrics-002	0.000	0.000	0.4 ± 0.03	41	0.408	35

Table 35. PA Type 8 (zoomed) - Use Case: detectImpersonationPA - Media Type: stills
(continued)

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
mbsolutions-000	0.000	0.000	0.42 ± 0.03	42	0.686	52
veridas-002	0.001	0.000	0.43 ± 0.03	43	0.883	64
griaule-001	0.000	0.000	0.55 ± 0.03	44	0.490	38
idvisioncenter-001	0.000	0.000	0.59 ± 0.03	45	0.902	67
cyberlink-002	0.000	0.000	0.6 ± 0.02	46	1.000	74
vida-001	0.001	0.000	0.61 ± 0.03	47	0.736	56
verigram-001	0.000	0.000	0.63 ± 0.03	48	0.614	46
visteam-002	0.000	0.000	0.66 ± 0.02	49	1.000	74
cyberlink-001	0.000	0.000	0.7 ± 0.02	50	0.761	59
mobbl-000	0.000	0.000	0.75 ± 0.02	51	0.580	45
techsign-001	0.000	0.007	0.79 ± 0.02	52	0.535	41
idvisioncenter-002	0.000	0.000	0.81 ± 0.02	53	0.893	65
techsign-000	0.000	0.000	0.81 ± 0.02	53	0.779	61
facedirect-001	0.000	0.000	0.82 ± 0.02	55	0.913	68
mobbl-001	0.000	0.000	0.87 ± 0.02	56	0.770	60
visteam-001	0.000	0.000	0.87 ± 0.02	57	0.934	69
biocube-002	0.000	0.000	0.88 ± 0.02	58	0.501	39
nsensekorea-001	0.000	0.000	0.89 ± 0.02	59	0.945	71
nsensekorea-000	0.000	0.000	0.89 ± 0.02	60	0.945	72
cubox-000	0.000	0.000	0.89 ± 0.02	61	0.806	62
biocube-001	0.000	0.000	0.91 ± 0.01	62	0.530	40
cubox-001	0.000	0.000	0.94 ± 0.01	63	0.893	65
spooff-000	0.000	0.000	0.94 ± 0.01	64	0.936	70
verigram-000	0.000	0.000	0.984 ± 0.007	65	0.462	36
tech5-001	0.007	0.002	0.993 ± 0.005	66	1.000	74
papago-001	0.000	0.000	0.999 ± 0.002	67	0.696	54
alchera-000	0.000	0.000	1 ± 0	68	1.000	74
alice-000	0.000	0.000	1 ± 0	68	0.813	63
aware-001	0.117	0.035	1 ± 0	68	0.248	22
facephi-000	0.000	0.000	1 ± 0	68	0.146	16
facephi-001	0.000	0.000	1 ± 0	68	0.079	11
griaule-000	0.000	0.000	1 ± 0	68	0.386	34
id3-001	0.000	0.000	1 ± 0	68	0.760	58
iproov-000	0.225	0.016	1 ± 0	68	0.046	9
neurotechnology-001	0.000	0.000	1 ± 0	68	0.224	20
pxl-000	0.002	0.000	1 ± 0	68	1.000	74
trueface-000	1.000	0.271	1 ± 0	68	0.272	24
uxlabs-001	0.000	0.000	1 ± 0	68	0.628	47
yoonik-001	0.000	0.000	1 ± 0	68	0.179	17
yoti-001	0.357	0.388	1 ± 0	68	0.688	53

Table 35. PA Type 8 (zoomed) - Use Case: detectImpersonationPA - Media Type: stills
(continued)

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
yoti-002	0.399	0.393	1 ± 0	68	0.745	57

Table 36. PA Type 1 - Use Case: detectImpersonationPA - Media Type: videos

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
cyberlink-002	0.000	0.000	0 ± 0	1	0.006	1
kakao-001	0.000	0.000	0 ± 0	1	0.006	1
cyberlink-001	0.000	0.000	0.1 ± 0.1	3	0.011	4
kakao-000	0.000	0.000	0.1 ± 0.1	3	0.041	11
stcon-001	0.000	0.000	0.1 ± 0.1	3	0.009	3
verihubs-inteligensia-001	0.000	0.000	0.1 ± 0.1	3	0.015	6
idrnd-001	0.000	0.000	0.1 ± 0.2	7	0.033	10
iproov-001	0.000	0.000	0.1 ± 0.2	7	0.071	15
kasikornlabs-000	0.000	0.000	0.1 ± 0.2	7	0.024	8
stcon-000	0.000	0.000	0.1 ± 0.2	7	0.188	28
idrnd-000	0.000	0.000	0.2 ± 0.2	11	0.087	18
veridas-001	0.000	0.000	0.2 ± 0.2	11	0.061	12
hyperverge-001	0.000	0.000	0.3 ± 0.2	13	0.149	24
kasikornlabs-001	0.000	0.000	0.3 ± 0.2	13	0.061	12
alice-001	0.000	0.000	0.3 ± 0.2	13	0.461	44
hyperverge-002	0.000	0.000	0.3 ± 0.2	13	0.022	7
veridas-002	0.000	0.000	0.3 ± 0.2	13	0.011	4
verihubs-inteligensia-000	0.000	0.000	0.3 ± 0.2	13	0.128	21
neurotechnology-000	0.000	0.000	0.4 ± 0.2	19	0.099	19
iidentifii-000	0.000	0.000	0.4 ± 0.3	20	0.171	25
facephi-000	0.000	0.000	0.5 ± 0.3	21	0.262	35
onfido-000	0.000	0.000	0.5 ± 0.3	21	0.788	68
meituan-000	0.000	0.000	0.6 ± 0.2	23	0.403	42
innovatrics-002	0.000	0.000	0.7 ± 0.2	24	0.608	54
rankone-000	0.000	0.000	0.7 ± 0.2	24	0.080	17
vida-001	0.000	0.000	0.7 ± 0.2	24	0.844	73
vida-002	0.000	0.000	0.7 ± 0.2	24	0.134	23
visteam-002	0.000	0.000	0.7 ± 0.2	24	0.065	14
meituan-001	0.000	0.000	0.7 ± 0.2	24	0.191	29
onfido-001	0.000	0.000	0.7 ± 0.2	24	0.753	66
techsign-000	0.000	0.000	0.7 ± 0.2	24	0.100	20
cubox-000	0.000	0.000	0.8 ± 0.2	32	0.489	46
facedirect-001	0.000	0.000	0.8 ± 0.2	32	0.770	67
id3-001	0.000	0.000	0.8 ± 0.2	32	0.221	33
idemia-010	0.000	0.000	0.8 ± 0.2	32	0.184	27
griaule-001	0.000	0.000	0.9 ± 0.1	36	0.214	31
idvisioncenter-001	0.000	0.000	0.9 ± 0.1	36	0.524	48
incode-001	0.000	0.000	0.9 ± 0.1	36	0.281	36
intema-000	0.000	0.000	0.9 ± 0.1	36	0.636	56
pxl-001	0.000	0.000	0.9 ± 0.1	36	0.130	22
saffe-002	0.000	0.000	0.9 ± 0.1	36	0.658	57

Table 36. PA Type 1 - Use Case: detectImpersonationPA - Media Type: videos (*continued*)

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
techsign-001	0.000	0.000	0.9 ± 0.1	36	0.325	39
verigram-000	0.000	0.000	0.9 ± 0.1	36	0.719	63
biocube-001	0.000	0.000	0.9 ± 0.2	44	0.483	45
biocube-002	0.000	0.000	0.9 ± 0.2	44	0.823	71
facephi-001	0.000	0.000	0.9 ± 0.2	44	0.664	58
idemia-011	0.000	0.000	0.9 ± 0.2	44	0.883	76
innovatrics-001	0.000	0.000	0.9 ± 0.2	44	0.680	61
intema-001	0.000	0.000	0.9 ± 0.2	44	0.621	55
alchera-000	0.000	0.000	1 ± 0	50	1.000	81
alice-000	0.000	0.000	1 ± 0	50	0.177	26
aware-001	0.000	0.004	1 ± 0	50	0.072	16
aware-002	0.000	0.000	1 ± 0	50	0.600	53
cubox-001	0.000	0.000	1 ± 0	50	0.305	37
facedirect-002	0.000	0.000	1 ± 0	50	0.991	78
griaule-000	0.000	0.000	1 ± 0	50	0.665	59
idvisioncenter-002	0.000	0.000	1 ± 0	50	0.554	50
incode-000	0.000	0.000	1 ± 0	50	0.309	38
iproov-000	0.000	0.017	1 ± 0	50	0.030	9
jcv-001	0.000	0.033	1 ± 0	50	0.513	47
jcv-002	0.000	0.013	1 ± 0	50	0.524	48
mbsolutions-000	0.000	0.000	1 ± 0	50	0.872	74
mbsolutions-001	0.000	0.000	1 ± 0	50	0.872	74
mobbl-000	0.000	0.000	1 ± 0	50	0.892	77
mobbl-001	0.000	0.000	1 ± 0	50	0.574	52
neurotechnology-001	0.000	0.000	1 ± 0	50	0.428	43
nsensekorea-000	0.000	0.000	1 ± 0	50	0.743	65
nsensekorea-001	0.000	0.000	1 ± 0	50	0.742	64
papago-001	0.000	0.000	1 ± 0	50	1.000	81
pxl-000	0.000	0.000	1 ± 0	50	0.998	79
rankone-001	0.000	0.000	1 ± 0	50	0.193	30
saffe-001	0.000	0.000	1 ± 0	50	0.797	70
spooff-000	0.000	0.000	1 ± 0	50	0.788	68
tech5-001	0.000	0.022	1 ± 0	50	0.998	79
trueface-000	0.267	0.803	1 ± 0	50	0.833	72
uxlabs-001	0.000	0.000	1 ± 0	50	0.567	51
verigram-001	0.000	0.000	1 ± 0	50	0.673	60
visteam-001	0.000	0.000	1 ± 0	50	0.712	62
younik-001	0.000	0.000	1 ± 0	50	0.387	40
younik-002	0.000	0.000	1 ± 0	50	0.390	41
yoti-001	0.400	0.160	1 ± 0	50	0.219	32
yoti-002	0.400	0.158	1 ± 0	50	0.240	34

Table 37. PA Type 3 - Use Case: detectImpersonationPA - Media Type: videos

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
alice-001	0	0.000	0 ± 0	1	0.002	1
cyberlink-001	0	0.000	0 ± 0	1	0.002	1
cyberlink-002	0	0.000	0 ± 0	1	0.002	1
idrnd-000	0	0.000	0 ± 0	1	0.002	1
idrnd-001	0	0.000	0 ± 0	1	0.002	1
iiidentifi-000	0	0.000	0 ± 0	1	0.002	1
incode-001	0	0.000	0 ± 0	1	0.002	1
innovatrics-002	0	0.000	0 ± 0	1	0.006	11
iproov-001	0	0.000	0 ± 0	1	0.002	1
stcon-000	0	0.000	0 ± 0	1	0.002	1
stcon-001	0	0.000	0 ± 0	1	0.002	1
facephi-000	0	0.000	0.1 ± 0.2	12	0.022	18
innovatrics-001	0	0.000	0.1 ± 0.2	12	0.188	39
kakao-001	0	0.000	0.1 ± 0.2	12	0.015	14
kasikornlabs-000	0	0.000	0.1 ± 0.2	12	0.013	12
kasikornlabs-001	0	0.000	0.1 ± 0.2	12	0.059	29
onfido-000	0	0.000	0.1 ± 0.2	12	0.013	12
onfido-001	0	0.000	0.1 ± 0.2	12	0.035	20
facephi-001	0	0.000	0.2 ± 0.2	19	0.046	25
rankone-000	0	0.000	0.2 ± 0.2	19	0.020	17
aware-002	0	0.000	0.3 ± 0.3	21	0.084	32
idemia-011	0	0.000	0.3 ± 0.3	21	0.041	22
incode-000	0	0.000	0.3 ± 0.3	21	0.033	19
intema-001	0	0.000	0.3 ± 0.3	21	0.119	36
mbsolutions-001	0	0.000	0.3 ± 0.3	21	0.658	54
meituan-000	0	0.000	0.3 ± 0.3	21	0.797	62
veridas-002	0	0.000	0.3 ± 0.3	21	0.043	23
intema-000	0	0.000	0.4 ± 0.3	28	0.374	49
neurotechnology-000	0	0.000	0.4 ± 0.3	28	0.139	38
saffe-002	0	0.000	0.4 ± 0.3	28	0.281	47
veridas-001	0	0.000	0.4 ± 0.3	28	0.128	37
vida-002	0	0.000	0.4 ± 0.3	28	0.232	45
griaule-000	0	0.000	0.5 ± 0.3	33	0.212	43
hyperverge-001	0	0.000	0.5 ± 0.3	33	0.112	34
kakao-000	0	0.000	0.5 ± 0.3	33	0.046	25
mbsolutions-000	0	0.000	0.5 ± 0.3	33	0.658	54
saffe-001	0	0.000	0.5 ± 0.3	33	0.214	44
idvisioncenter-001	0	0.000	0.6 ± 0.3	38	0.901	69
vida-001	0	0.000	0.6 ± 0.3	38	0.361	48
facedirect-001	0	0.000	0.7 ± 0.3	40	0.045	24
meituan-001	0	0.000	0.7 ± 0.3	40	0.050	27

Table 37. PA Type 3 - Use Case: detectImpersonationPA - Media Type: videos (*continued*)

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
rankone-001	0	0.000	0.7 ± 0.3	40	0.037	21
visteam-002	0	0.000	0.7 ± 0.3	40	0.058	28
idemia-010	0	0.000	0.8 ± 0.2	44	0.117	35
techsign-001	0	0.000	0.8 ± 0.2	44	0.104	33
verihubs-inteligensia-000	0	0.000	0.8 ± 0.2	44	0.600	52
biocube-001	0	0.000	0.9 ± 0.2	47	0.797	62
biocube-002	0	0.000	0.9 ± 0.2	47	0.901	69
griaule-001	0	0.000	0.9 ± 0.2	47	0.203	42
hyperverge-002	0	0.000	0.9 ± 0.2	47	0.069	31
id3-001	0	0.000	0.9 ± 0.2	47	0.883	68
idvisioncenter-002	0	0.000	0.9 ± 0.2	47	0.688	57
techsign-000	0	0.000	0.9 ± 0.2	47	0.753	60
verihubs-inteligensia-001	0	0.000	0.9 ± 0.2	47	0.266	46
alchera-000	0	0.000	1 ± 0	55	0.998	77
alice-000	0	0.000	1 ± 0	55	0.063	30
aware-001	0	0.004	1 ± 0	55	0.017	15
cupbox-000	0	0.000	1 ± 0	55	0.976	74
cupbox-001	0	0.000	1 ± 0	55	0.998	77
facedirect-002	0	0.000	1 ± 0	55	0.991	76
iproov-000	0	0.017	1 ± 0	55	0.017	15
jcv-001	0	0.033	1 ± 0	55	1.000	81
jcv-002	0	0.013	1 ± 0	55	0.727	58
mobbl-000	0	0.000	1 ± 0	55	0.913	71
mobbl-001	0	0.000	1 ± 0	55	0.814	66
neurotechnology-001	0	0.000	1 ± 0	55	0.643	53
nsensekorea-000	0	0.000	1 ± 0	55	0.998	77
nsensekorea-001	0	0.000	1 ± 0	55	0.998	77
papago-001	0	0.000	1 ± 0	55	1.000	81
pxl-000	0	0.000	1 ± 0	55	0.955	73
pxl-001	0	0.000	1 ± 0	55	0.680	56
spooff-000	0	0.000	1 ± 0	55	0.833	67
tech5-001	0	0.022	1 ± 0	55	0.976	74
trueface-000	1	0.803	1 ± 0	55	0.805	64
uxlabs-001	0	0.000	1 ± 0	55	0.561	51
verigram-000	0	0.000	1 ± 0	55	0.805	64
verigram-001	0	0.000	1 ± 0	55	0.530	50
visteam-001	0	0.000	1 ± 0	55	0.924	72
younik-001	0	0.000	1 ± 0	55	0.762	61
younik-002	0	0.000	1 ± 0	55	0.743	59
yoti-001	0	0.160	1 ± 0	55	0.191	41
yoti-002	0	0.158	1 ± 0	55	0.188	39

Table 38. PA Type 8 - Use Case: detectImpersonationPA - Media Type: videos

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
alice-001	0.000	0.000	0 ± 0	1	0.002	1
cyberlink-002	0.000	0.000	0 ± 0	1	0.004	23
facephi-000	0.000	0.000	0 ± 0	1	0.002	1
facephi-001	0.000	0.000	0 ± 0	1	0.002	1
griaule-000	0.000	0.000	0 ± 0	1	0.002	1
hyperverge-001	0.000	0.000	0 ± 0	1	0.002	1
hyperverge-002	0.000	0.000	0 ± 0	1	0.006	26
idemia-011	0.000	0.000	0 ± 0	1	0.002	1
idrnd-000	0.000	0.000	0 ± 0	1	0.002	1
idrnd-001	0.000	0.000	0 ± 0	1	0.002	1
idvisioncenter-001	0.000	0.000	0 ± 0	1	0.006	26
iidentifi-000	0.000	0.000	0 ± 0	1	0.002	1
intema-000	0.000	0.000	0 ± 0	1	0.002	1
intema-001	0.000	0.000	0 ± 0	1	0.002	1
iproov-001	0.000	0.000	0 ± 0	1	0.002	1
kasikornlabs-000	0.000	0.000	0 ± 0	1	0.002	1
kasikornlabs-001	0.000	0.000	0 ± 0	1	0.002	1
mbsolutions-000	0.000	0.000	0 ± 0	1	0.007	29
mbsolutions-001	0.000	0.000	0 ± 0	1	0.002	1
meituan-000	0.000	0.000	0 ± 0	1	0.002	1
meituan-001	0.000	0.000	0 ± 0	1	0.002	1
neurotechnology-000	0.000	0.000	0 ± 0	1	0.002	1
onfido-000	0.000	0.000	0 ± 0	1	0.004	23
saffe-001	0.000	0.000	0 ± 0	1	0.002	1
saffe-002	0.000	0.000	0 ± 0	1	0.002	1
stcon-000	0.000	0.000	0 ± 0	1	0.002	1
stcon-001	0.000	0.000	0 ± 0	1	0.002	1
verigram-001	0.000	0.000	0 ± 0	1	0.006	26
vida-002	0.000	0.000	0 ± 0	1	0.004	23
cyberlink-001	0.000	0.000	0.02 ± 0.03	30	0.032	39
incode-001	0.000	0.000	0.02 ± 0.03	30	0.019	34
innovatrics-001	0.000	0.000	0.02 ± 0.03	30	0.022	37
onfido-001	0.000	0.000	0.02 ± 0.03	30	0.011	31
rankone-001	0.000	0.000	0.02 ± 0.03	30	0.009	30
kakao-001	0.000	0.000	0.04 ± 0.05	35	0.052	43
idemia-010	0.000	0.000	0.07 ± 0.06	36	0.048	42
innovatrics-002	0.000	0.000	0.07 ± 0.06	36	0.019	34
id3-001	0.000	0.000	0.11 ± 0.08	38	0.046	41
kakao-000	0.000	0.000	0.11 ± 0.08	38	0.165	59
incode-000	0.000	0.000	0.13 ± 0.08	40	0.015	32
verigram-000	0.000	0.000	0.13 ± 0.09	41	0.052	43

Table 38. PA Type 8 - Use Case: detectImpersonationPA - Media Type: videos (*continued*)

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
techsign-001	0.000	0.000	0.2 ± 0.1	42	0.149	56
verihubs-inteligensia-000	0.000	0.000	0.2 ± 0.1	42	0.262	65
verihubs-inteligensia-001	0.000	0.000	0.2 ± 0.1	42	0.227	62
yoonik-001	0.000	0.000	0.3 ± 0.1	45	0.084	50
pxl-001	0.000	0.000	0.4 ± 0.1	46	0.078	48
rankone-000	0.000	0.000	0.4 ± 0.1	46	0.024	38
idvisioncenter-002	0.000	0.000	0.4 ± 0.1	46	0.045	40
veridas-001	0.000	0.000	0.5 ± 0.1	49	0.067	47
griaule-001	0.000	0.000	0.5 ± 0.1	49	0.104	54
visteam-001	0.000	0.000	0.5 ± 0.1	49	0.574	72
facedirect-002	0.000	0.000	0.6 ± 0.1	52	0.991	78
facedirect-001	0.000	0.000	0.7 ± 0.1	53	0.987	77
veridas-002	0.000	0.000	0.7 ± 0.1	53	0.086	51
techsign-000	0.000	0.000	0.7 ± 0.1	53	0.082	49
aware-002	0.000	0.000	0.8 ± 0.1	56	0.309	67
vida-001	0.000	0.000	0.8 ± 0.1	56	0.234	63
biocube-001	0.000	0.000	0.8 ± 0.1	56	0.600	73
biocube-002	0.000	0.000	0.8 ± 0.1	56	0.554	71
nsensekorea-000	0.000	0.000	0.8 ± 0.1	56	0.409	69
nsensekorea-001	0.000	0.000	0.8 ± 0.1	56	0.418	70
mobbl-000	0.000	0.000	0.89 ± 0.08	62	0.892	76
visteam-002	0.000	0.000	0.91 ± 0.08	63	0.257	64
cubox-001	0.000	0.000	0.96 ± 0.05	64	0.385	68
mobbl-001	0.000	0.000	0.96 ± 0.05	64	0.703	74
alchera-000	0.000	0.000	1 ± 0	66	1.000	80
alice-000	0.000	0.000	1 ± 0	66	0.065	46
aware-001	0.000	0.004	1 ± 0	66	0.143	55
cubox-000	0.000	0.000	1 ± 0	66	0.095	53
iproov-000	0.000	0.017	1 ± 0	66	0.017	33
jcv-001	0.037	0.033	1 ± 0	66	0.059	45
jcv-002	0.019	0.013	1 ± 0	66	0.019	34
neurotechnology-001	0.000	0.000	1 ± 0	66	0.154	58
papago-001	0.000	0.000	1 ± 0	66	1.000	80
pxl-000	0.000	0.000	1 ± 0	66	1.000	80
spooff-000	0.000	0.000	1 ± 0	66	0.307	66
tech5-001	0.037	0.022	1 ± 0	66	0.998	79
trueface-000	0.704	0.803	1 ± 0	66	0.805	75
uxlabs-001	0.000	0.000	1 ± 0	66	0.093	52
yoonik-002	0.000	0.000	1 ± 0	66	0.149	56
yoti-001	0.037	0.160	1 ± 0	66	0.201	60
yoti-002	0.037	0.158	1 ± 0	66	0.208	61

Fig. 12. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

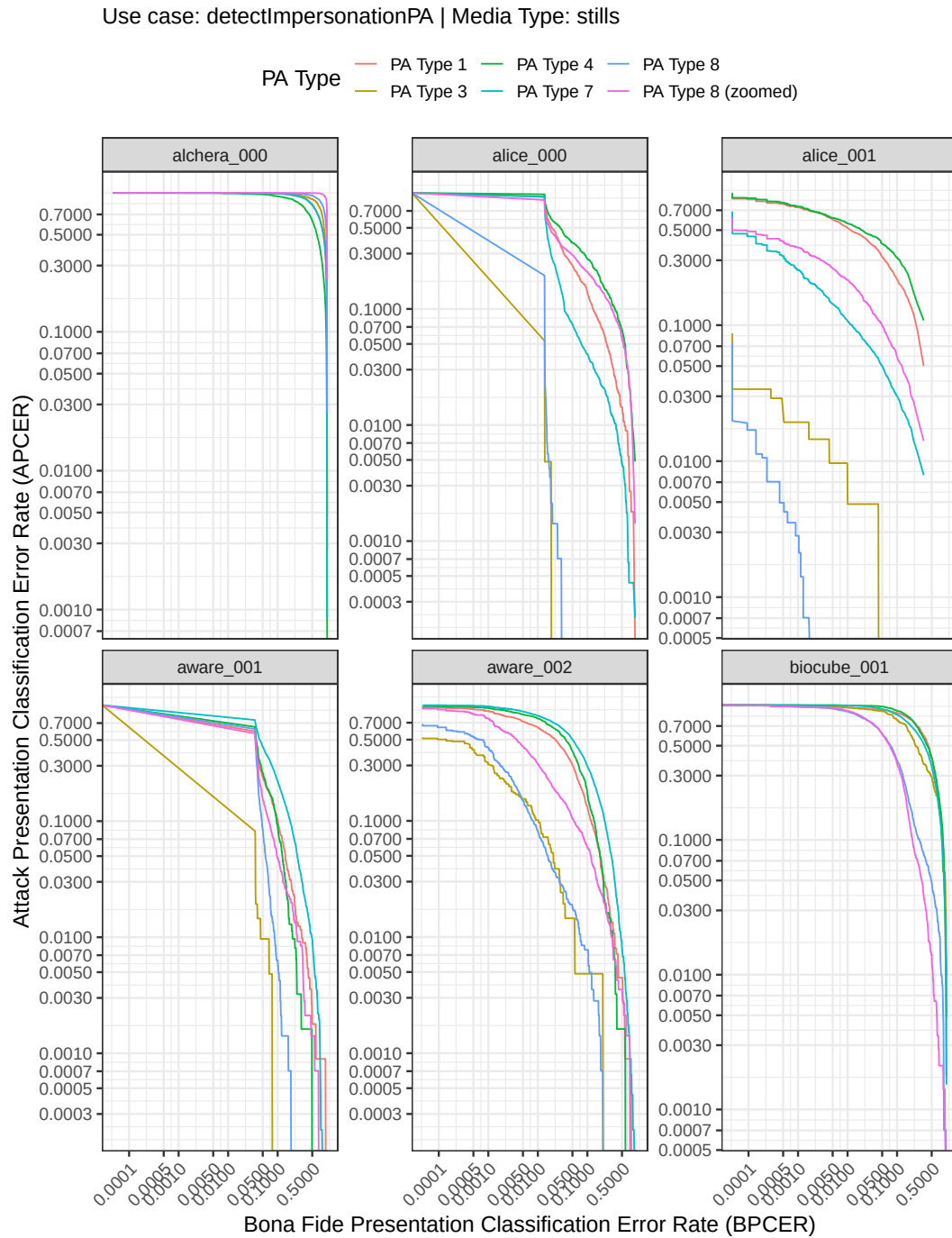


Fig. 13. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

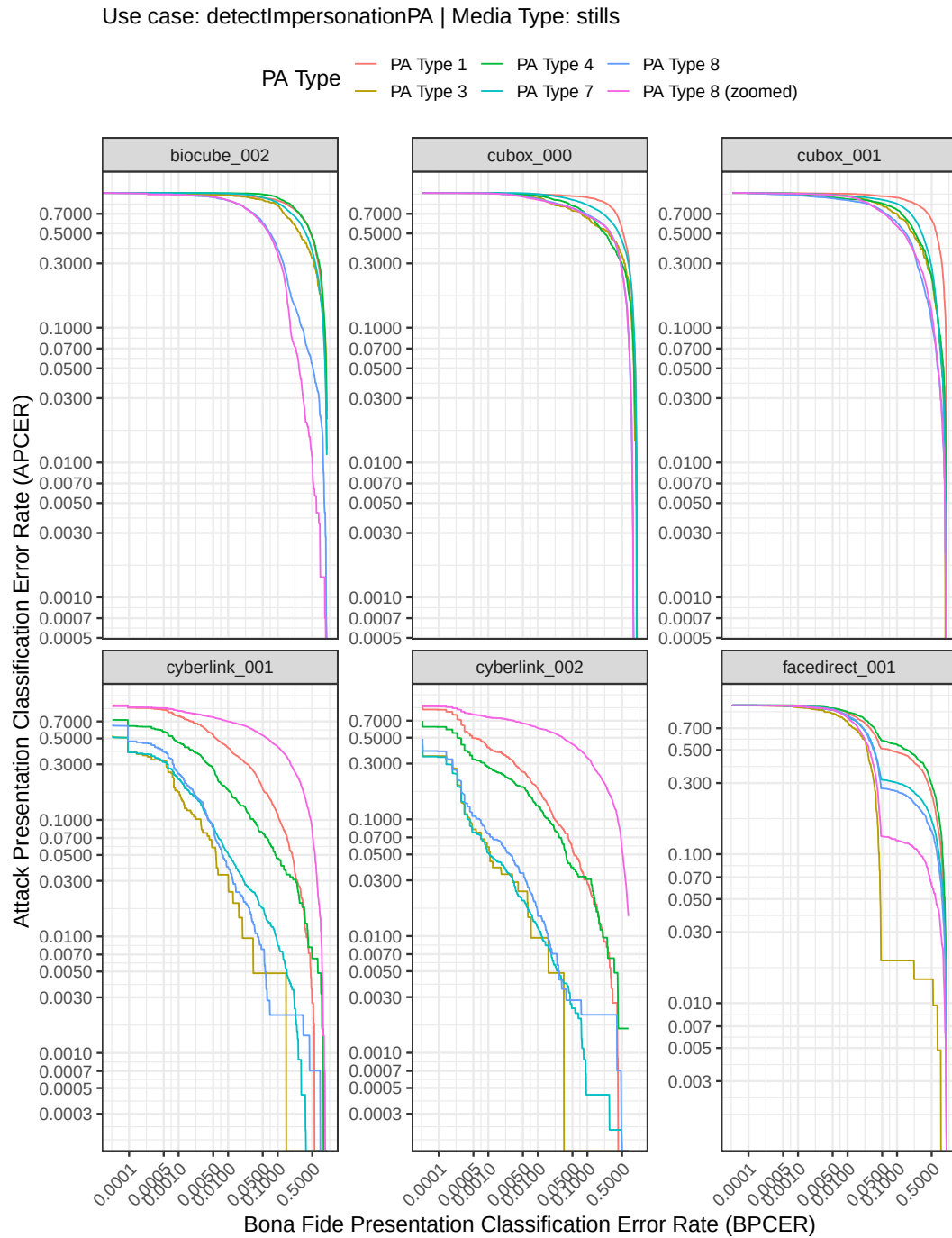


Fig. 14. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

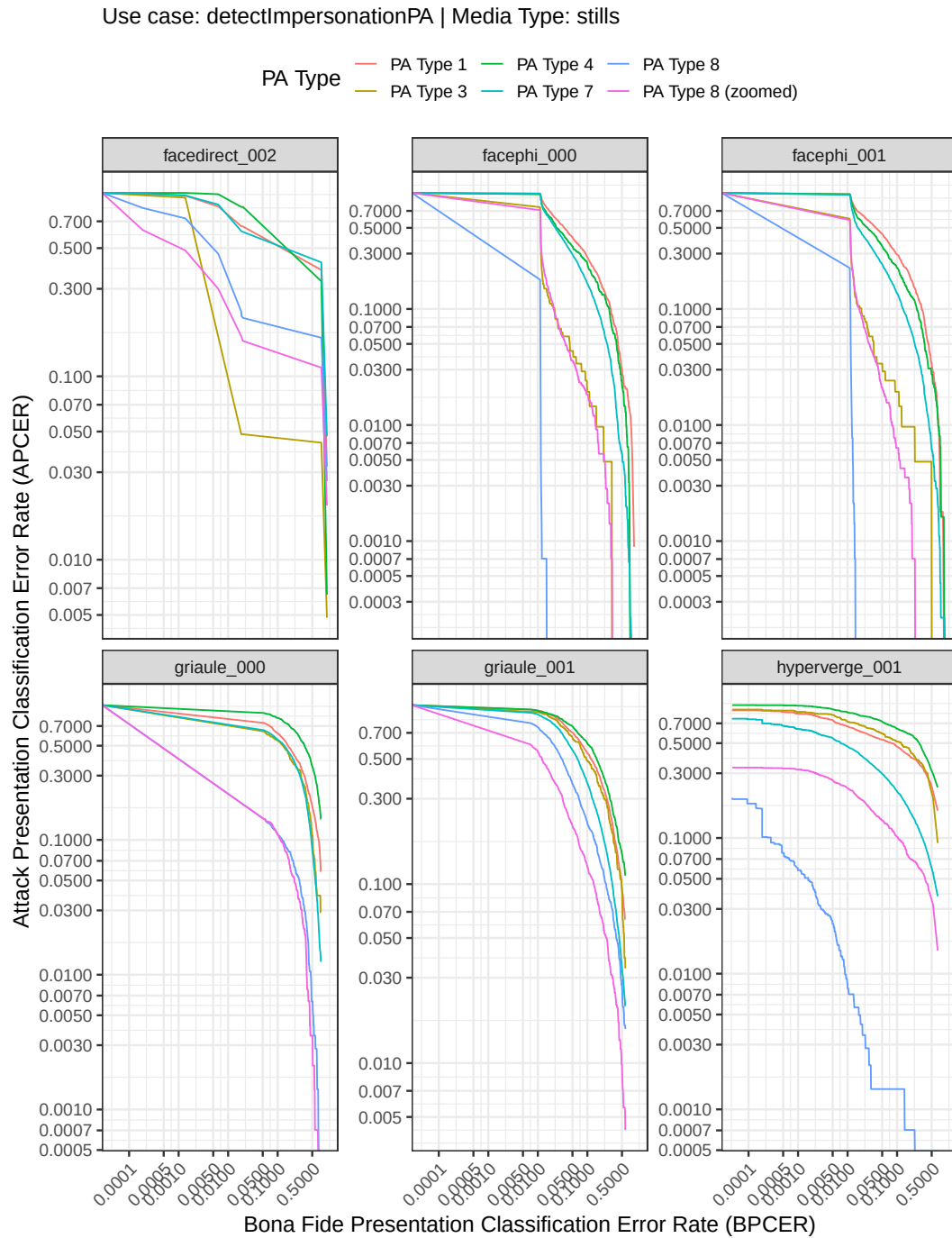


Fig. 15. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

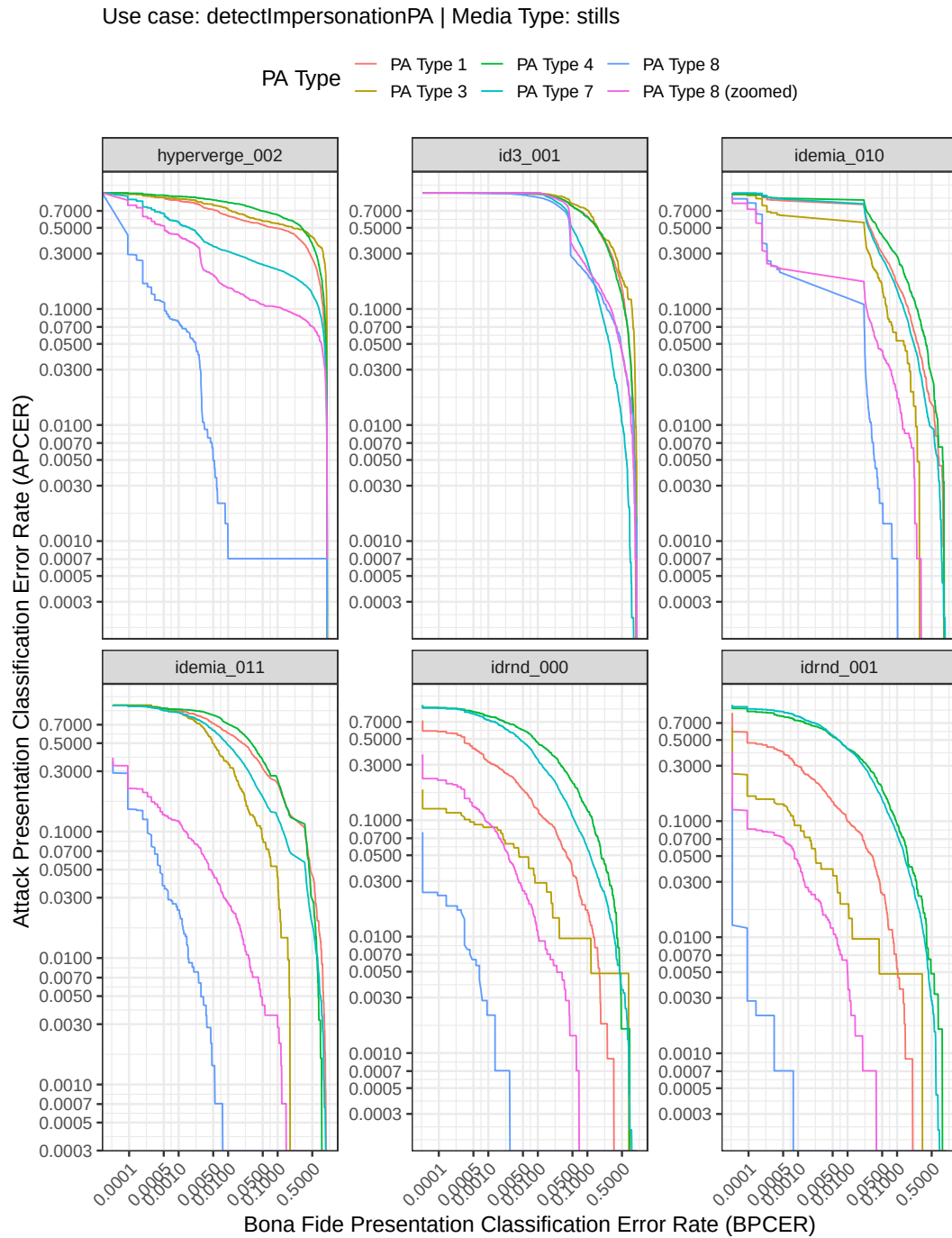


Fig. 16. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

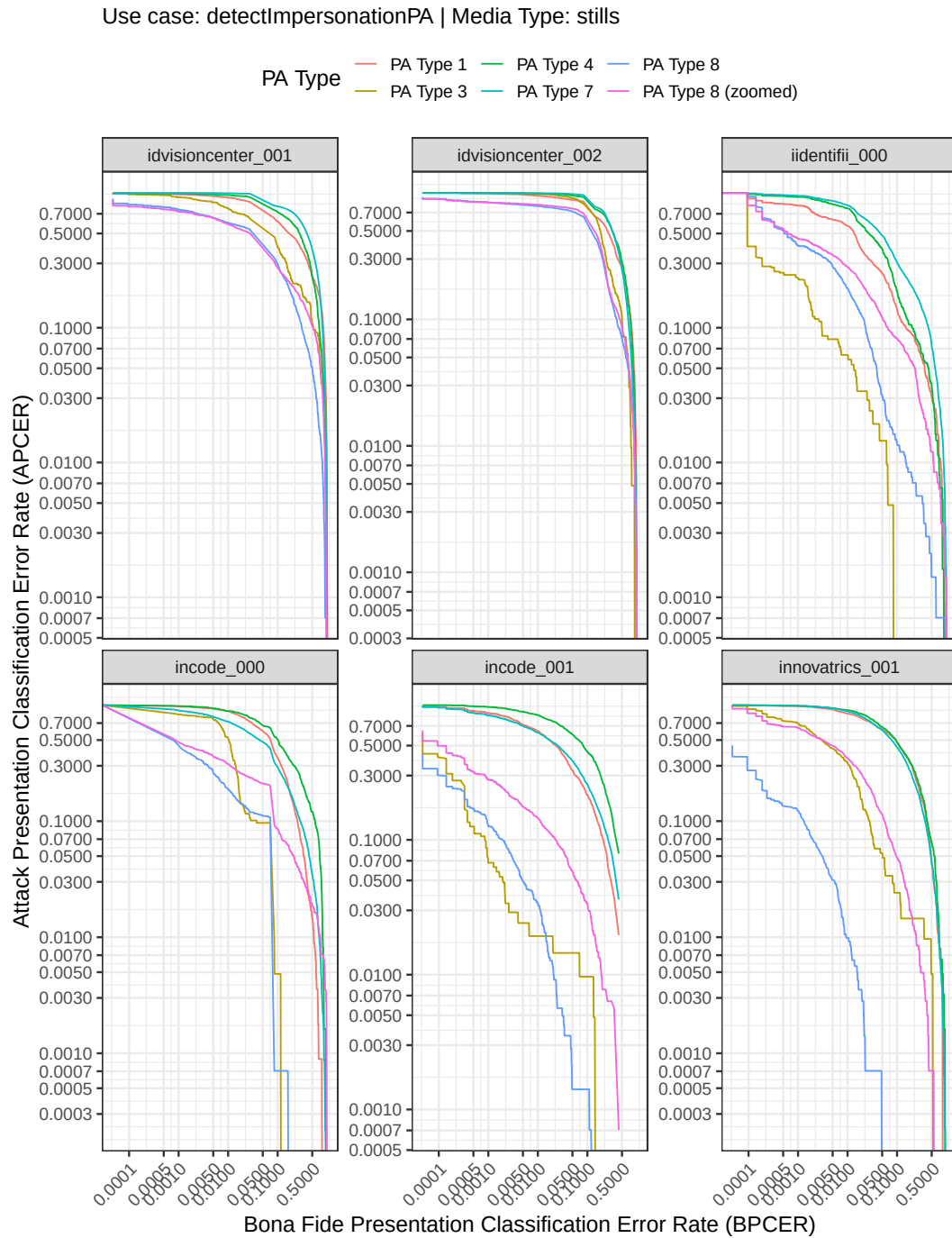


Fig. 17. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

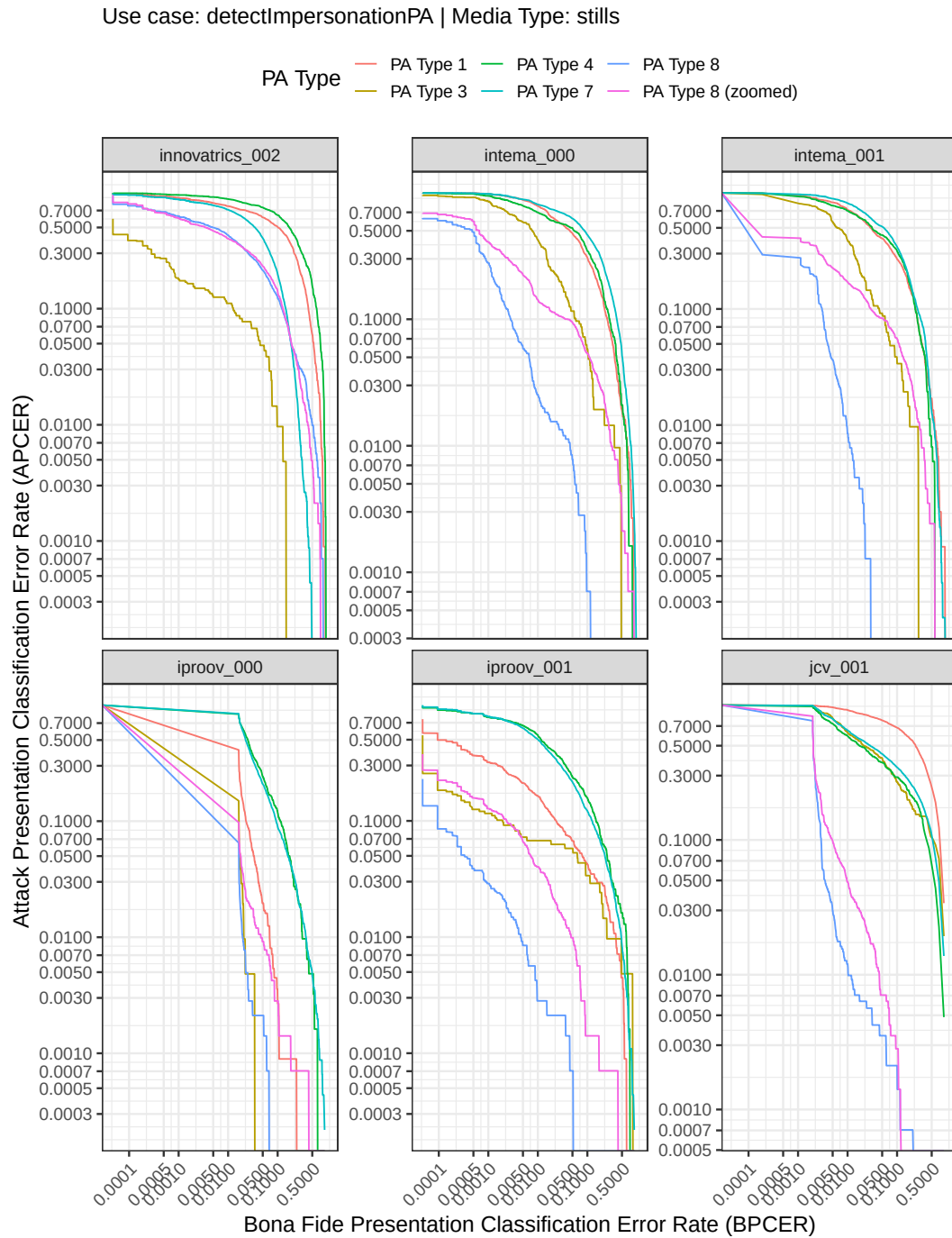


Fig. 18. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

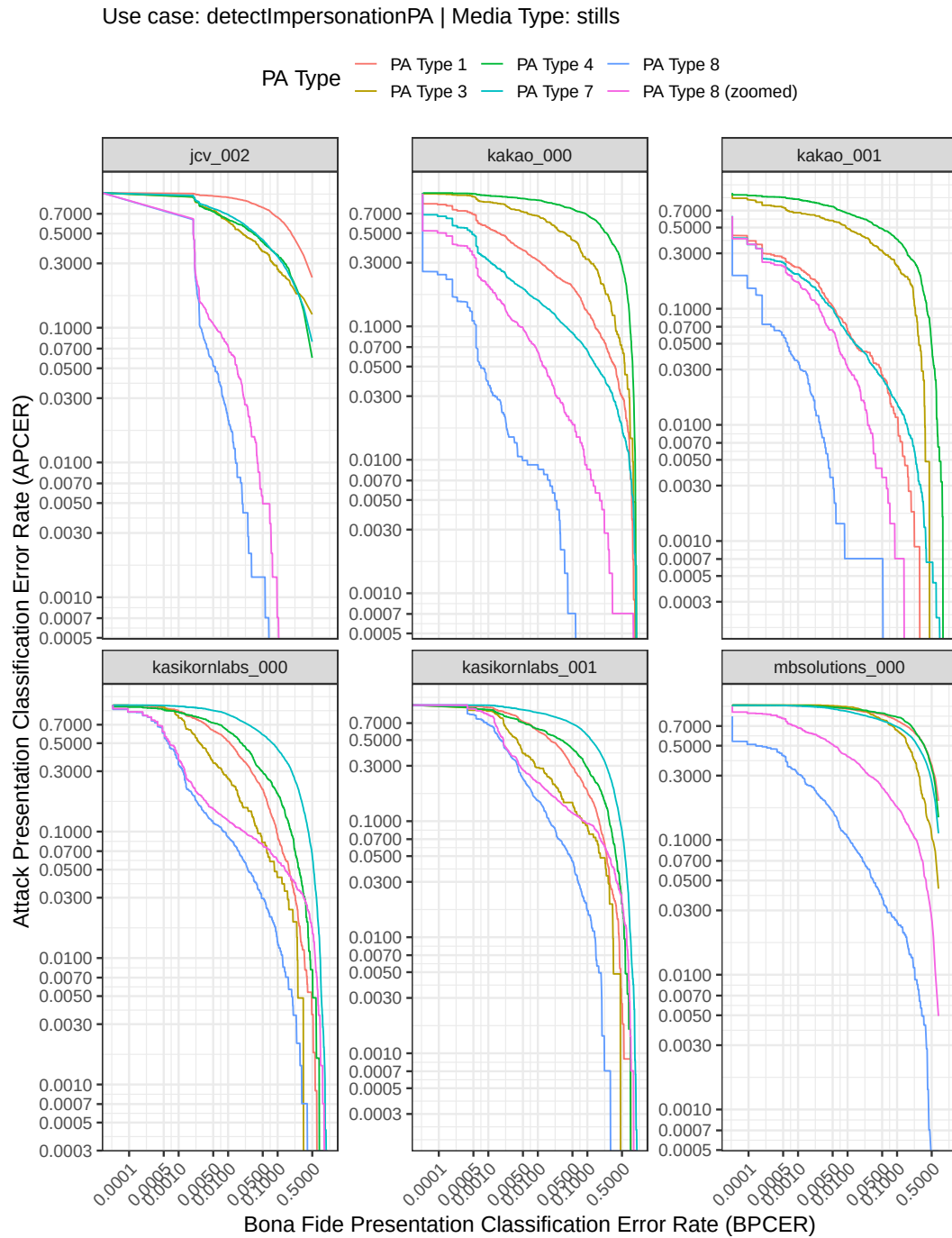


Fig. 19. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

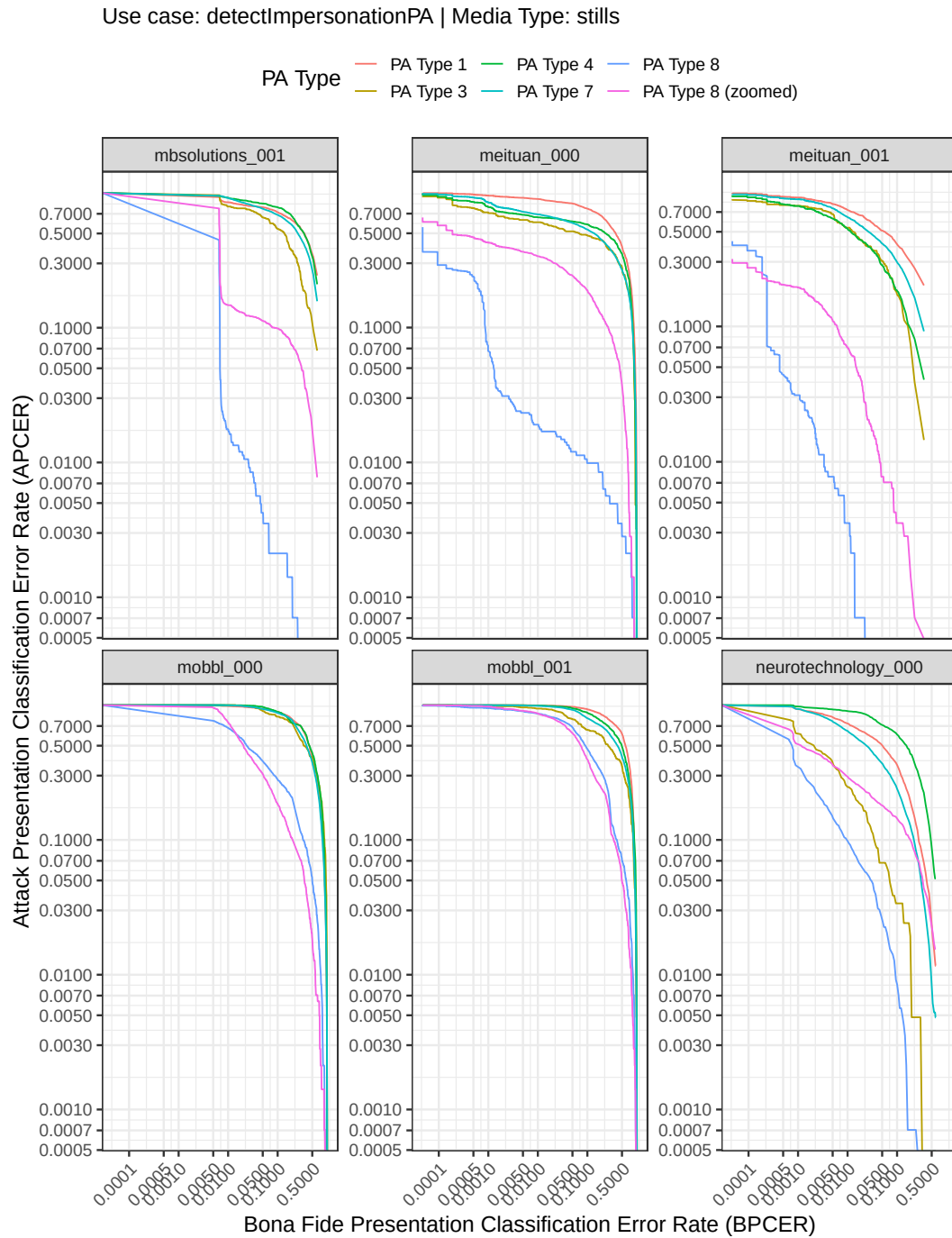


Fig. 20. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

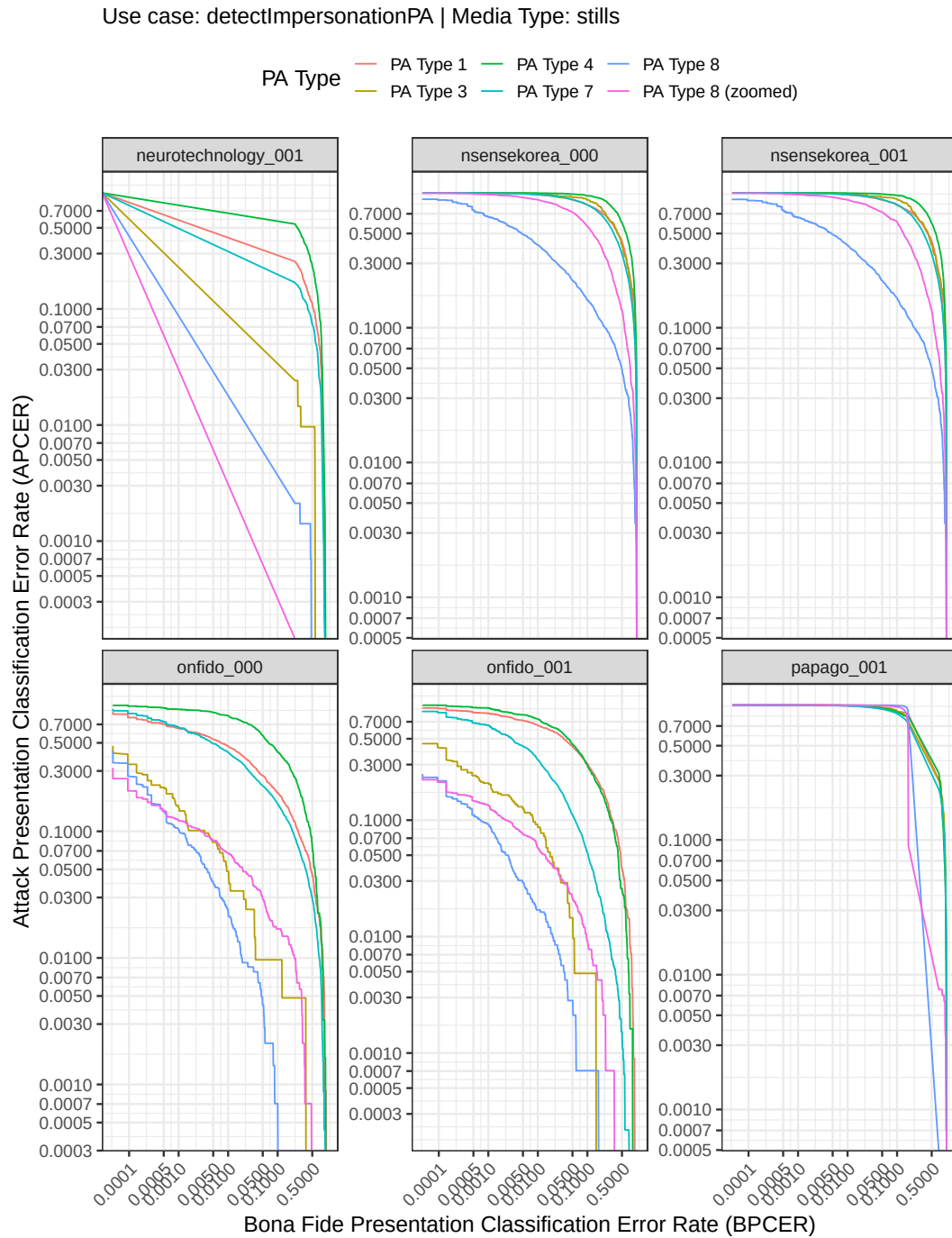


Fig. 21. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

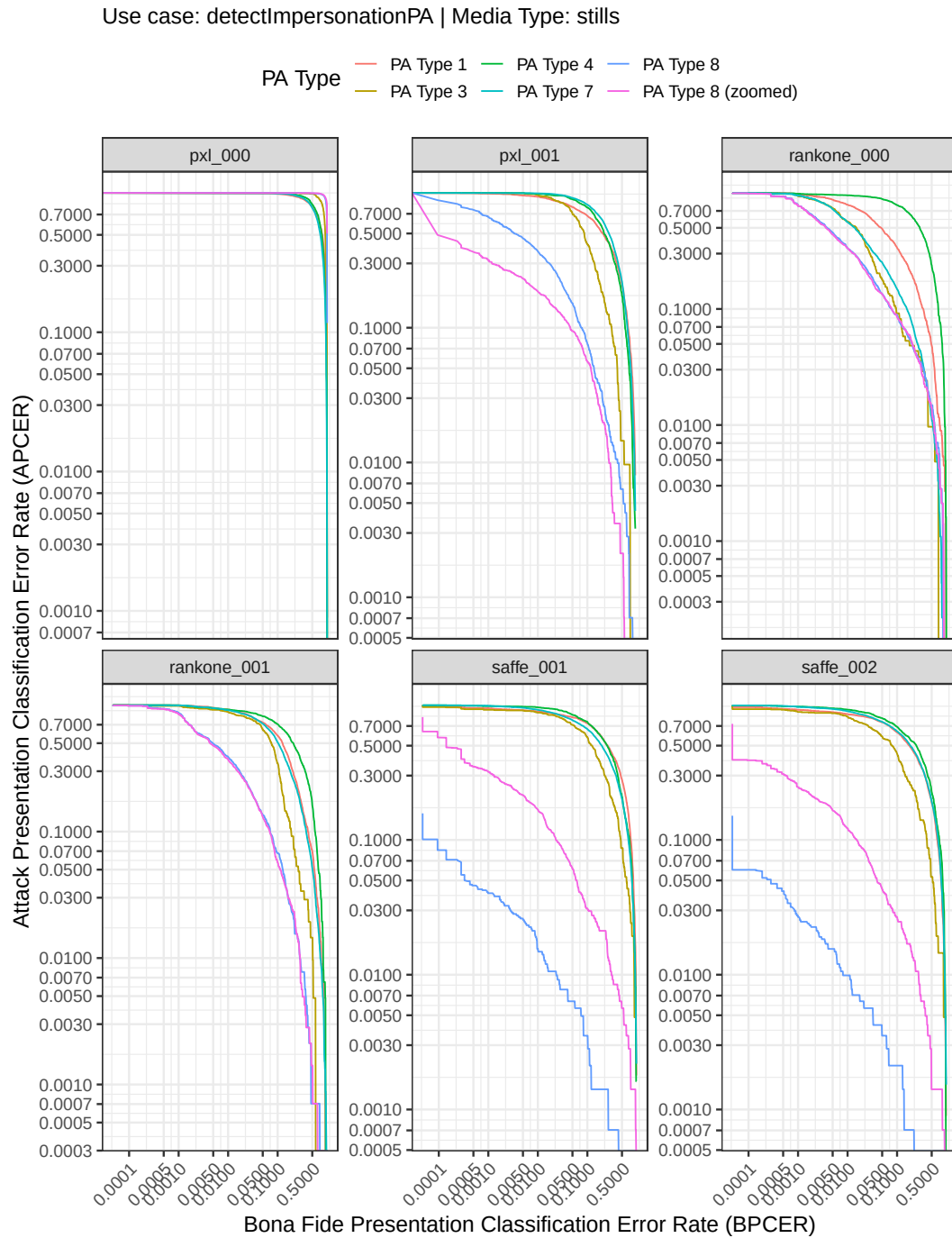


Fig. 22. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

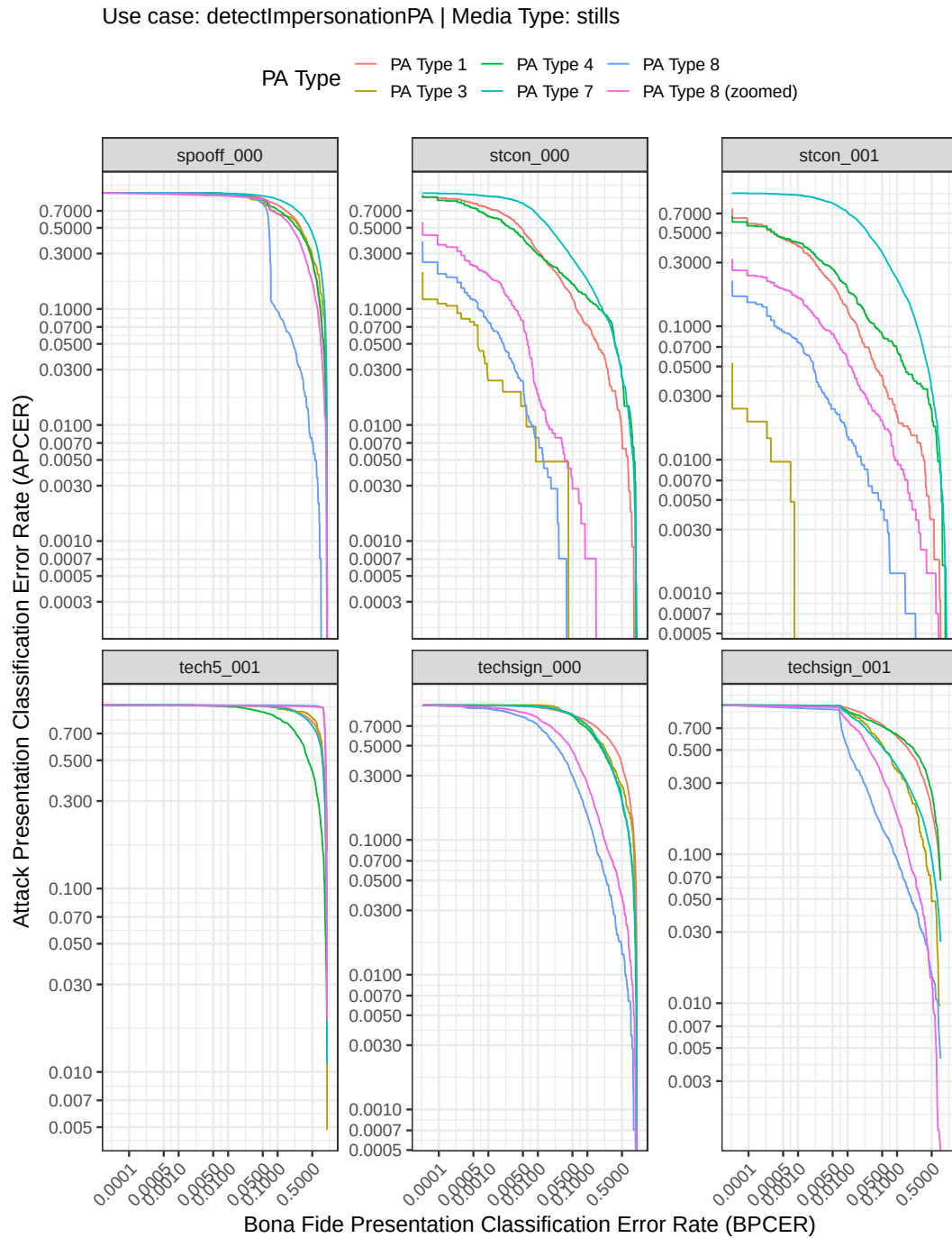


Fig. 23. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

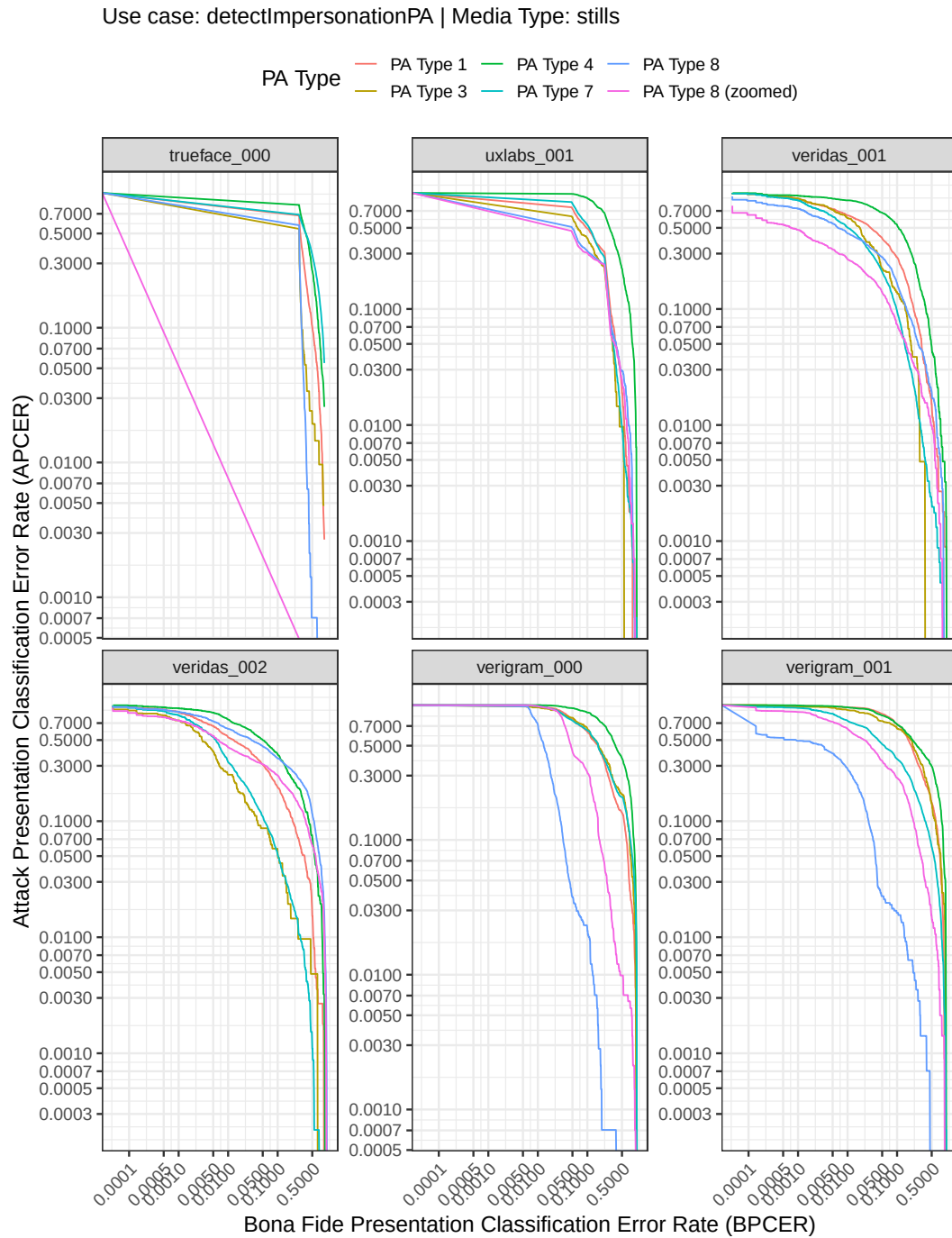


Fig. 24. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

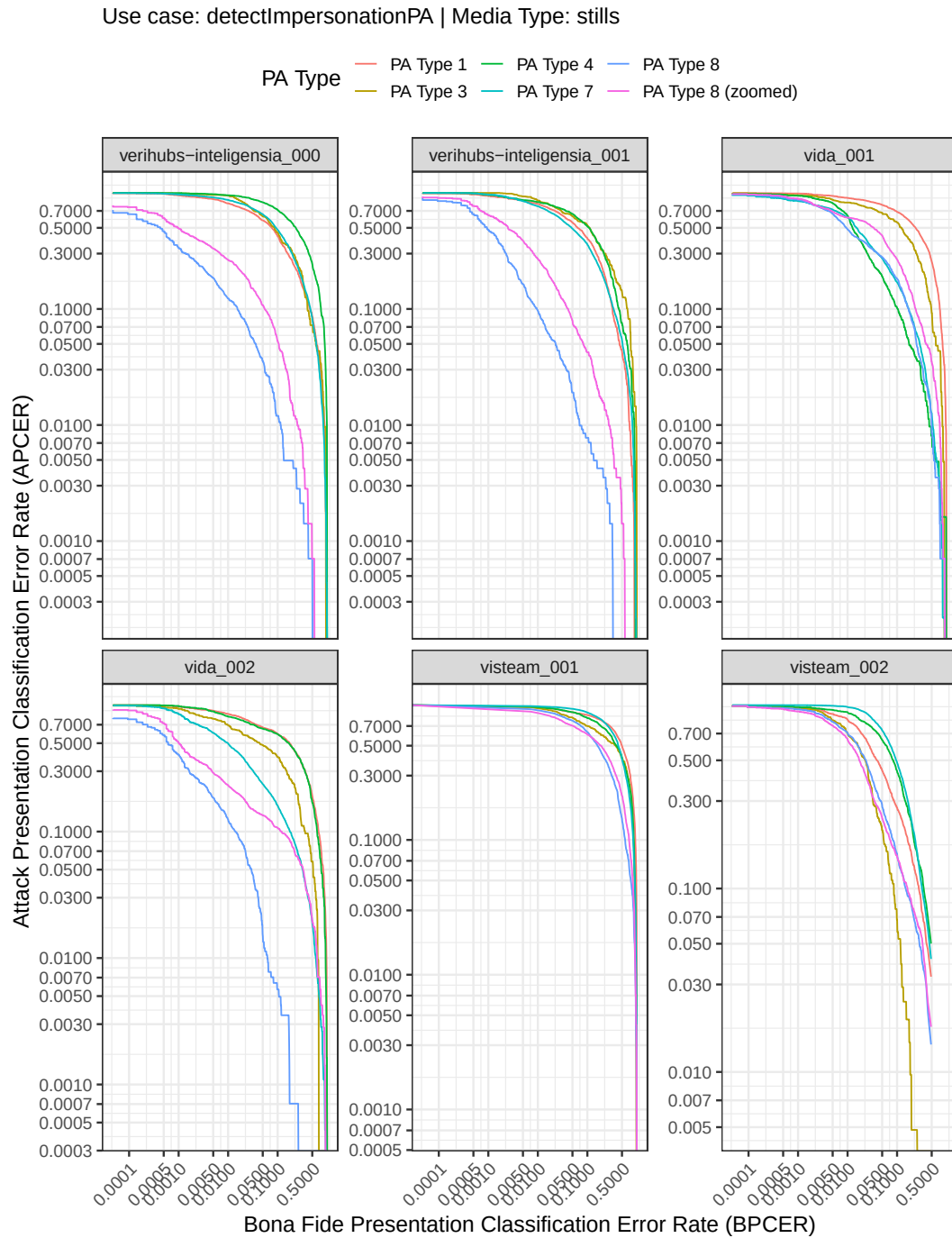


Fig. 25. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA stills.

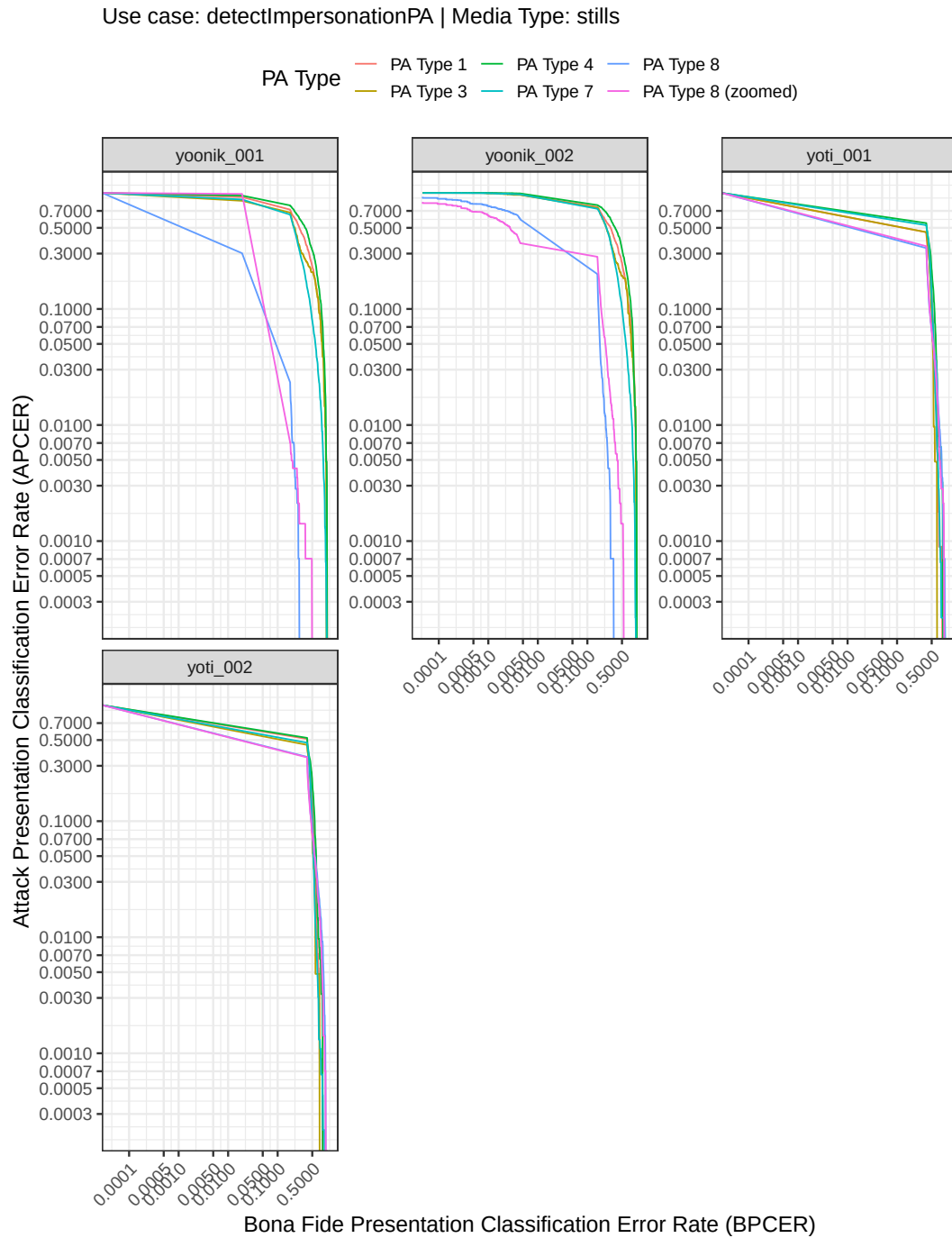


Fig. 26. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

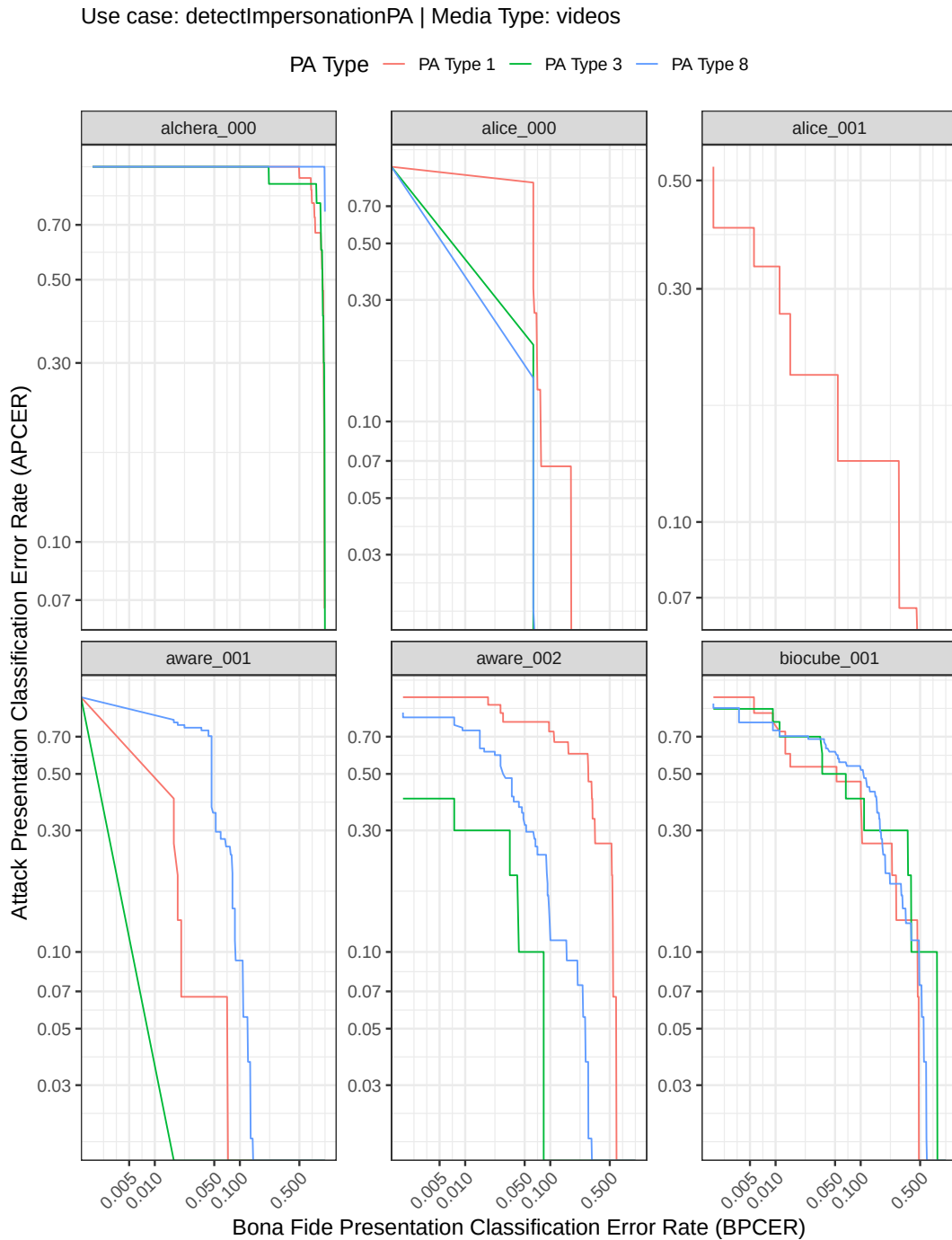


Fig. 27. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

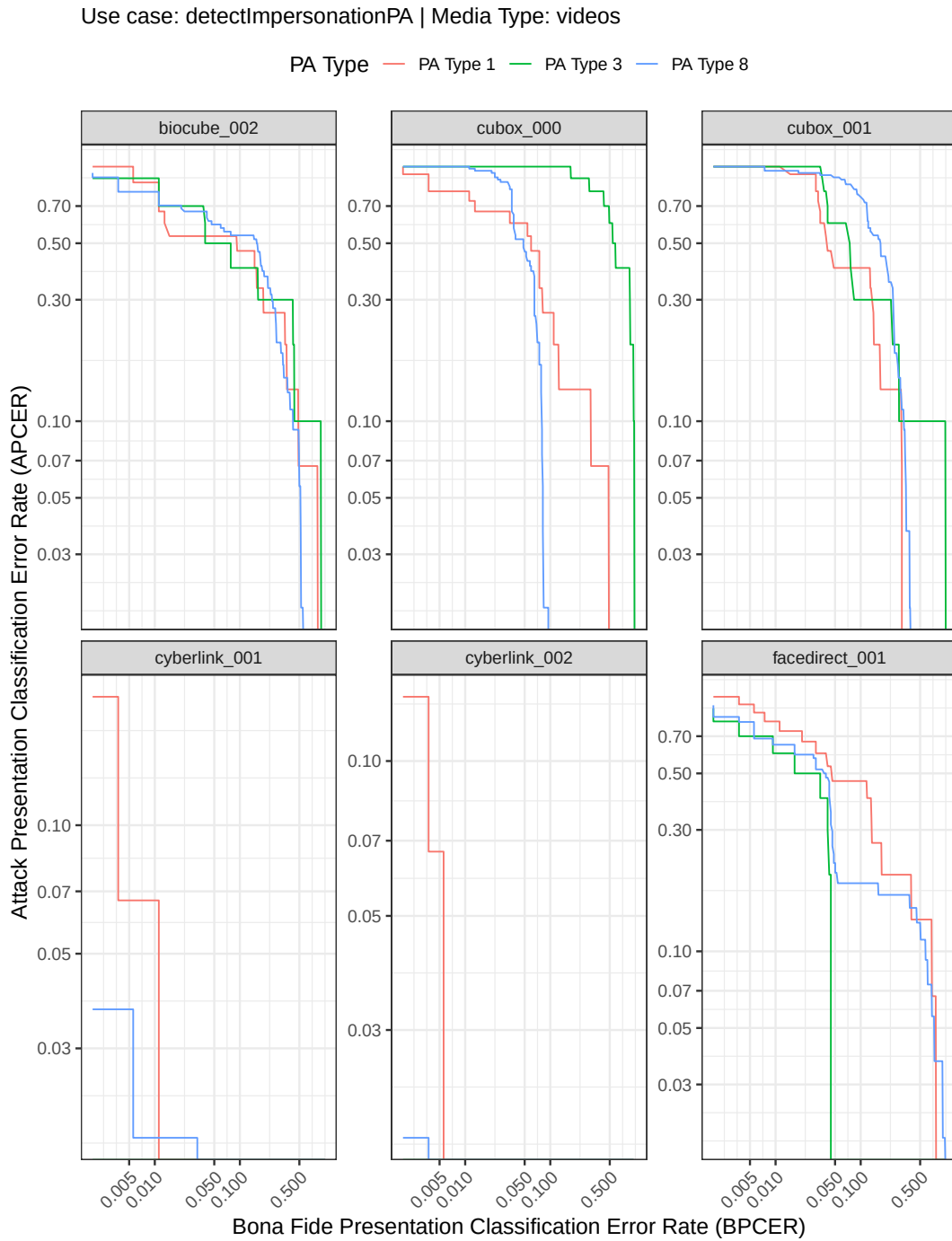


Fig. 28. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

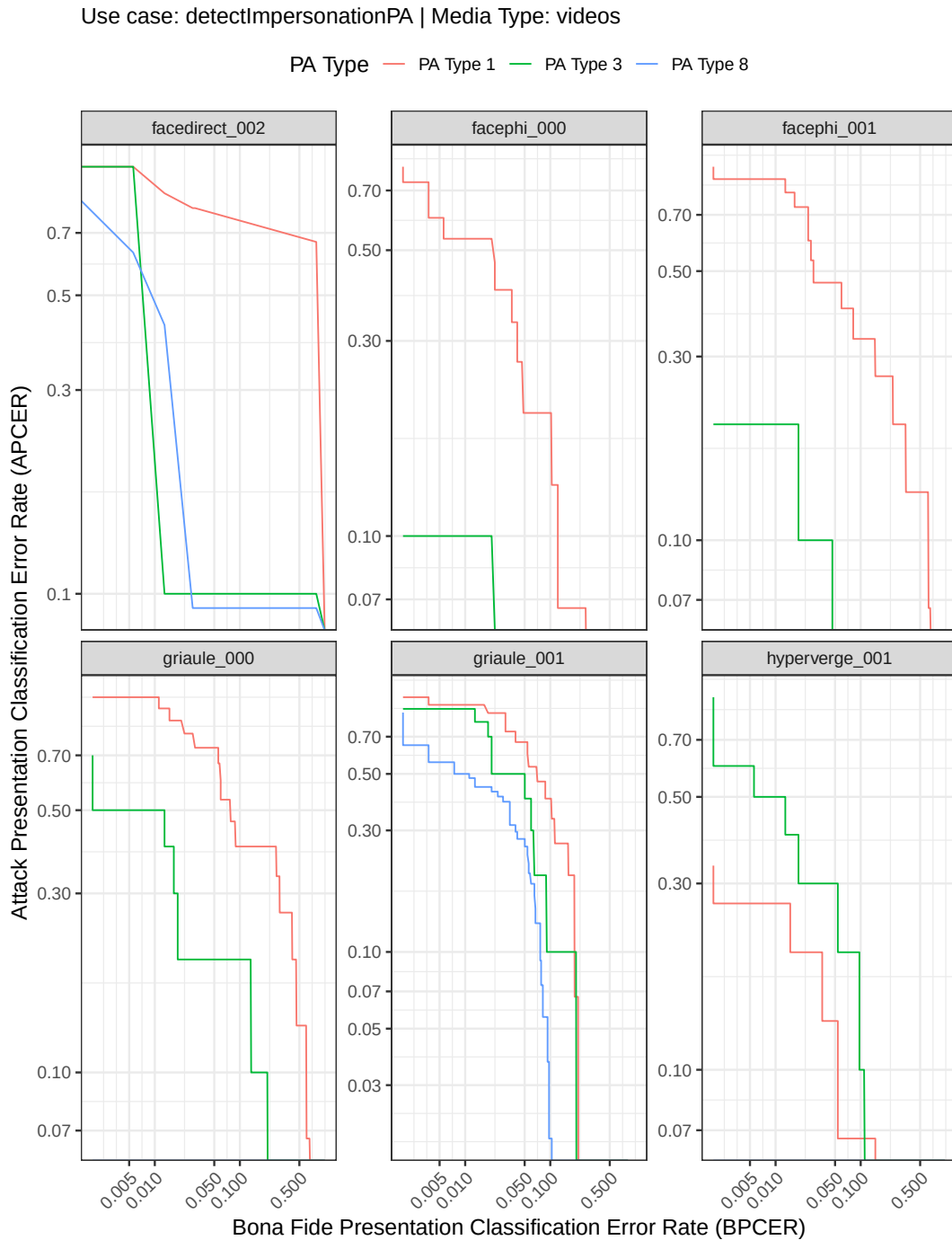


Fig. 29. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

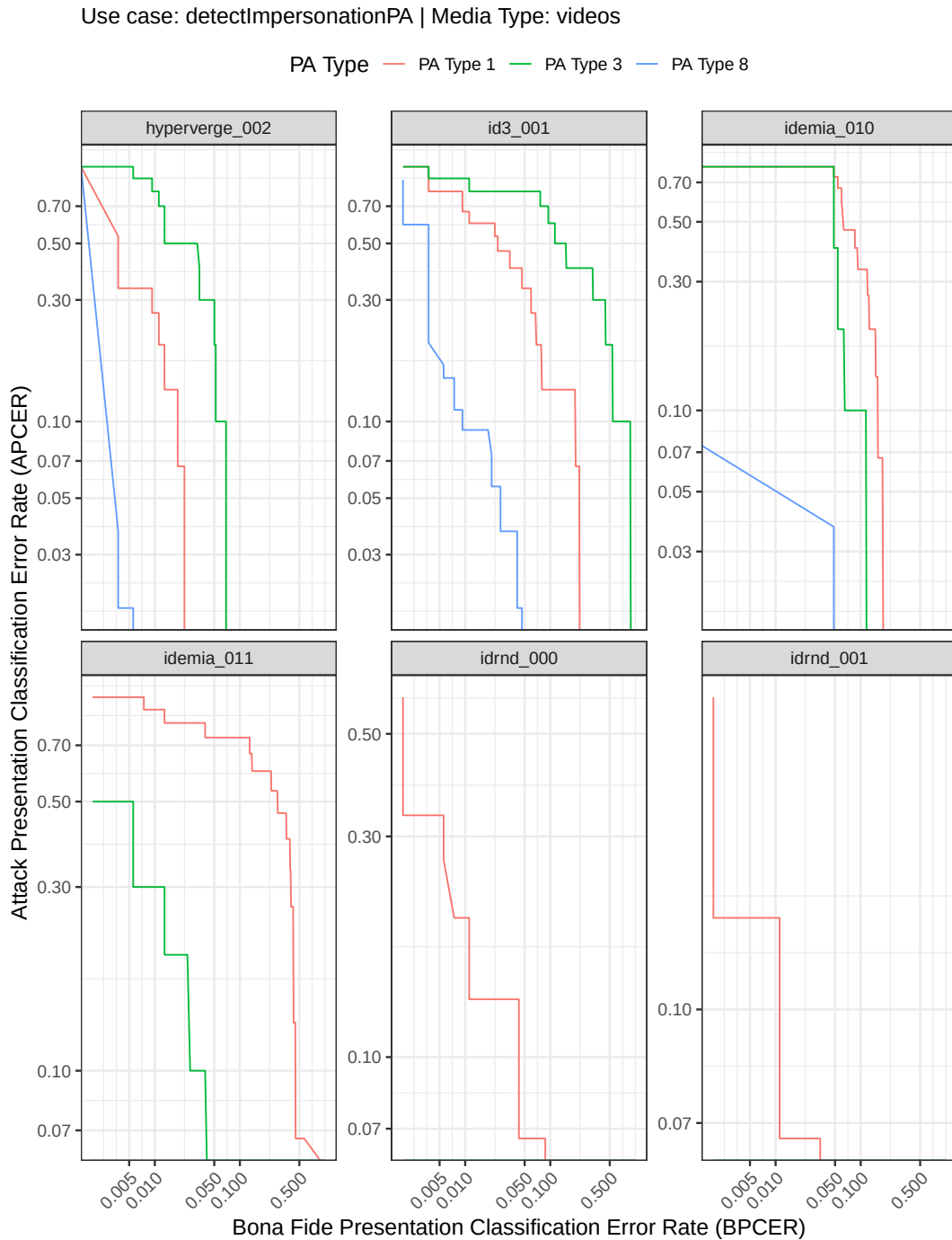


Fig. 30. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

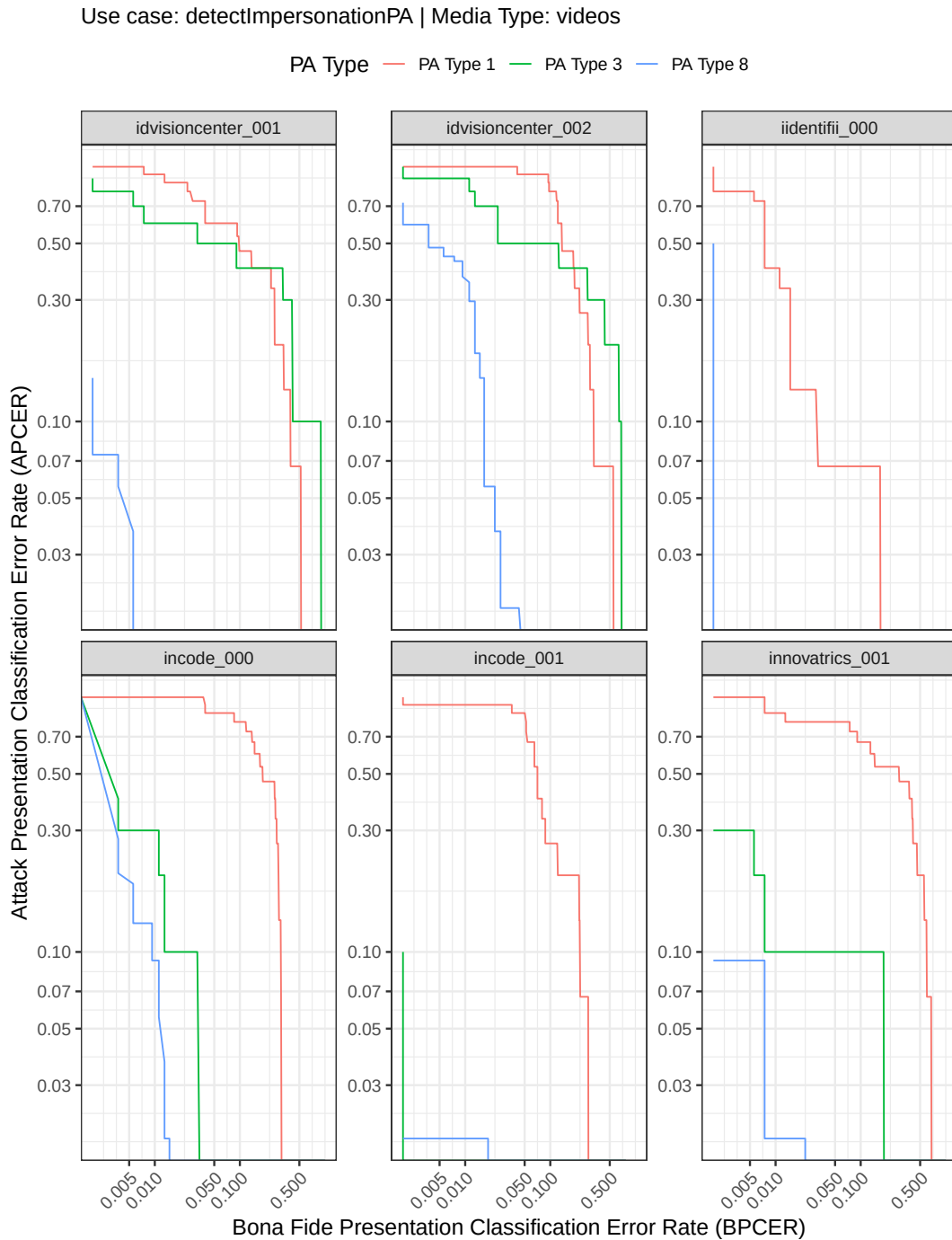


Fig. 31. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

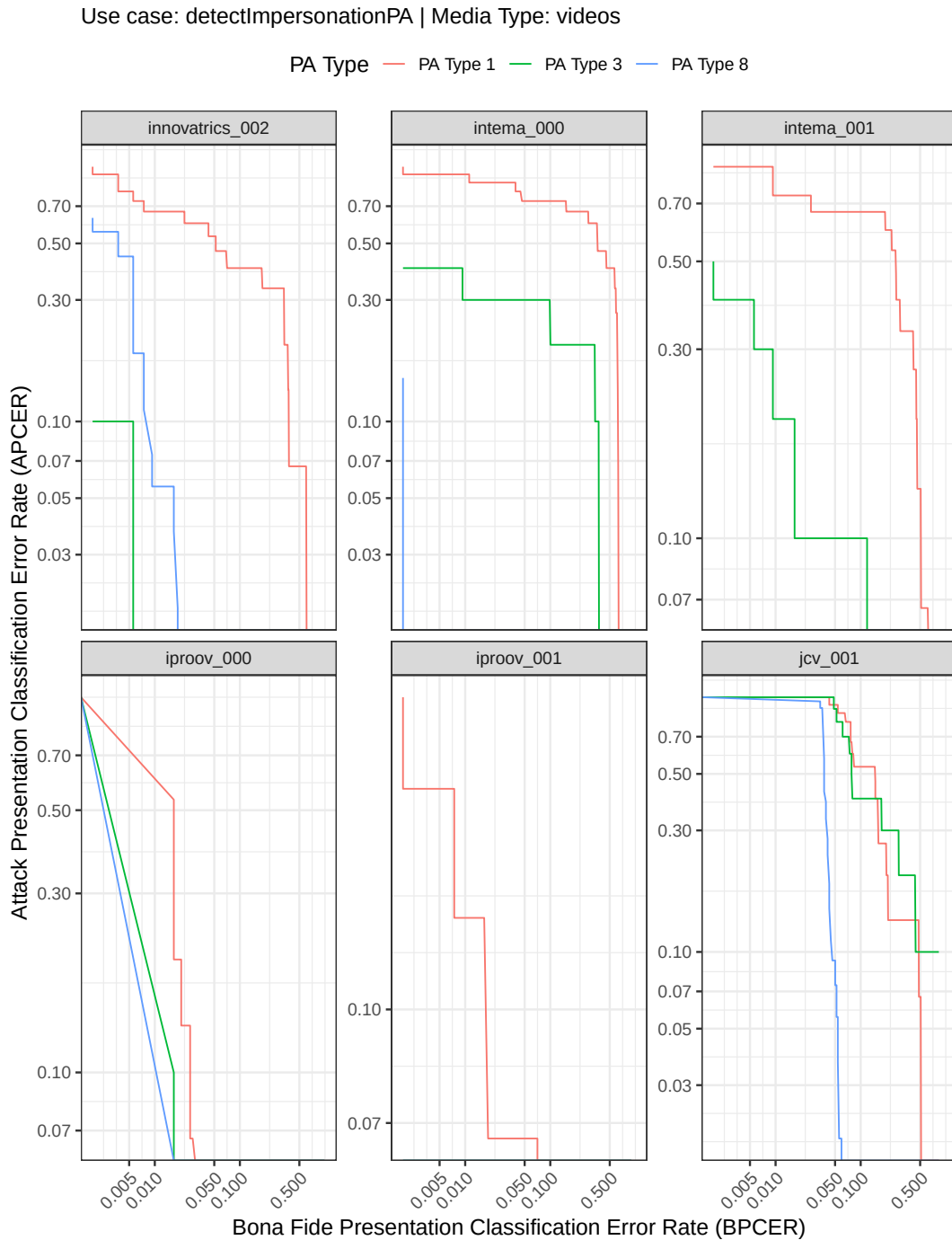


Fig. 32. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

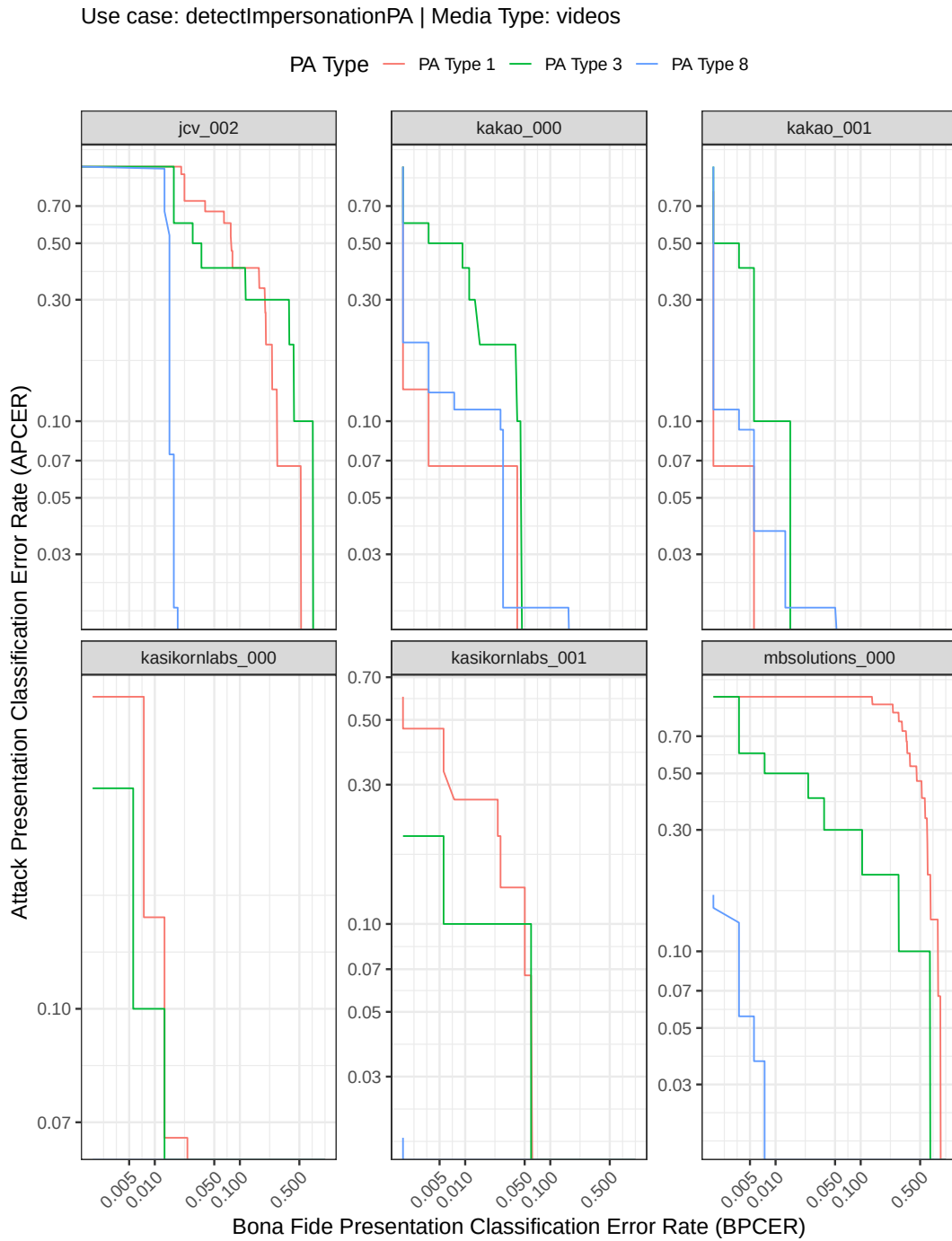


Fig. 33. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

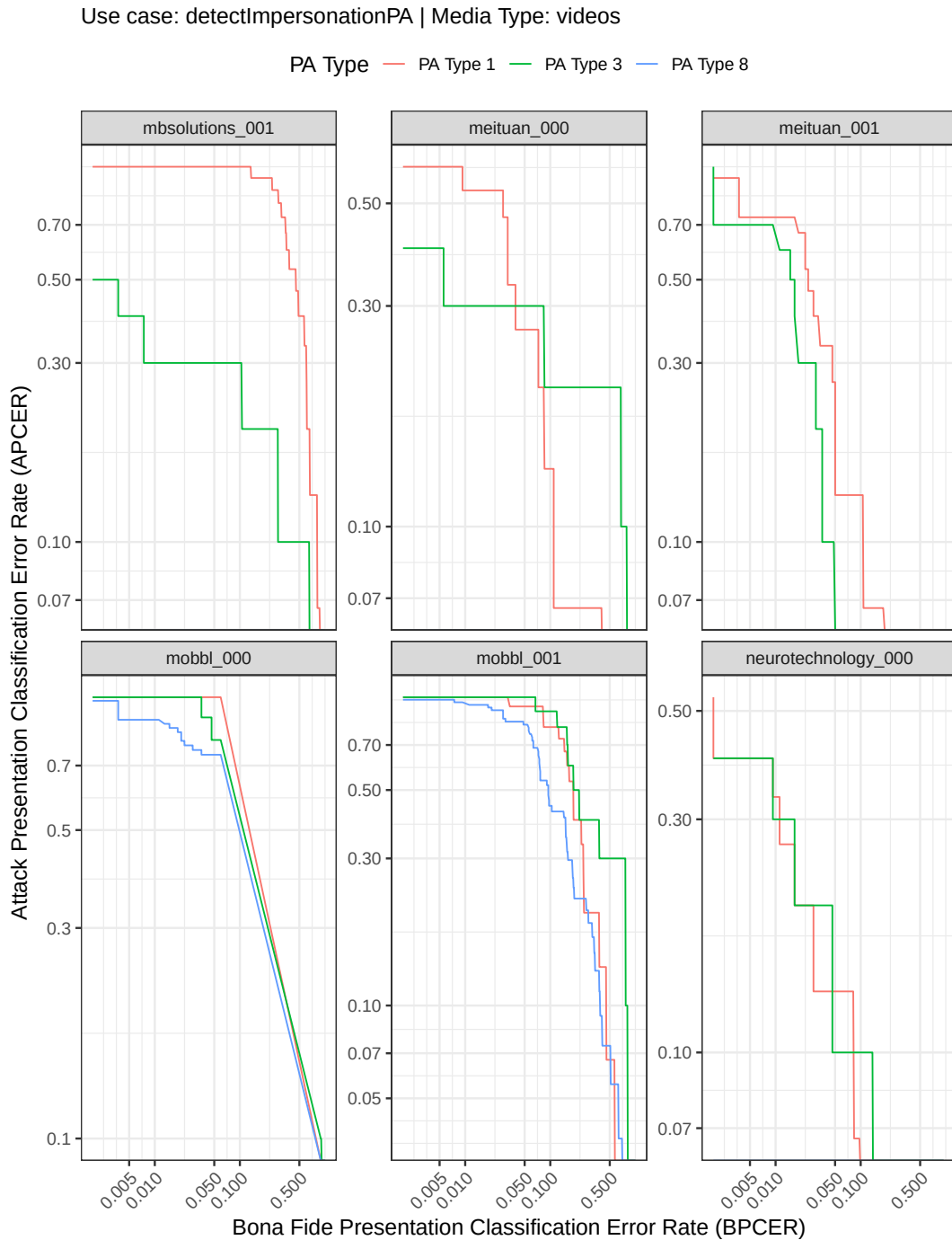


Fig. 34. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

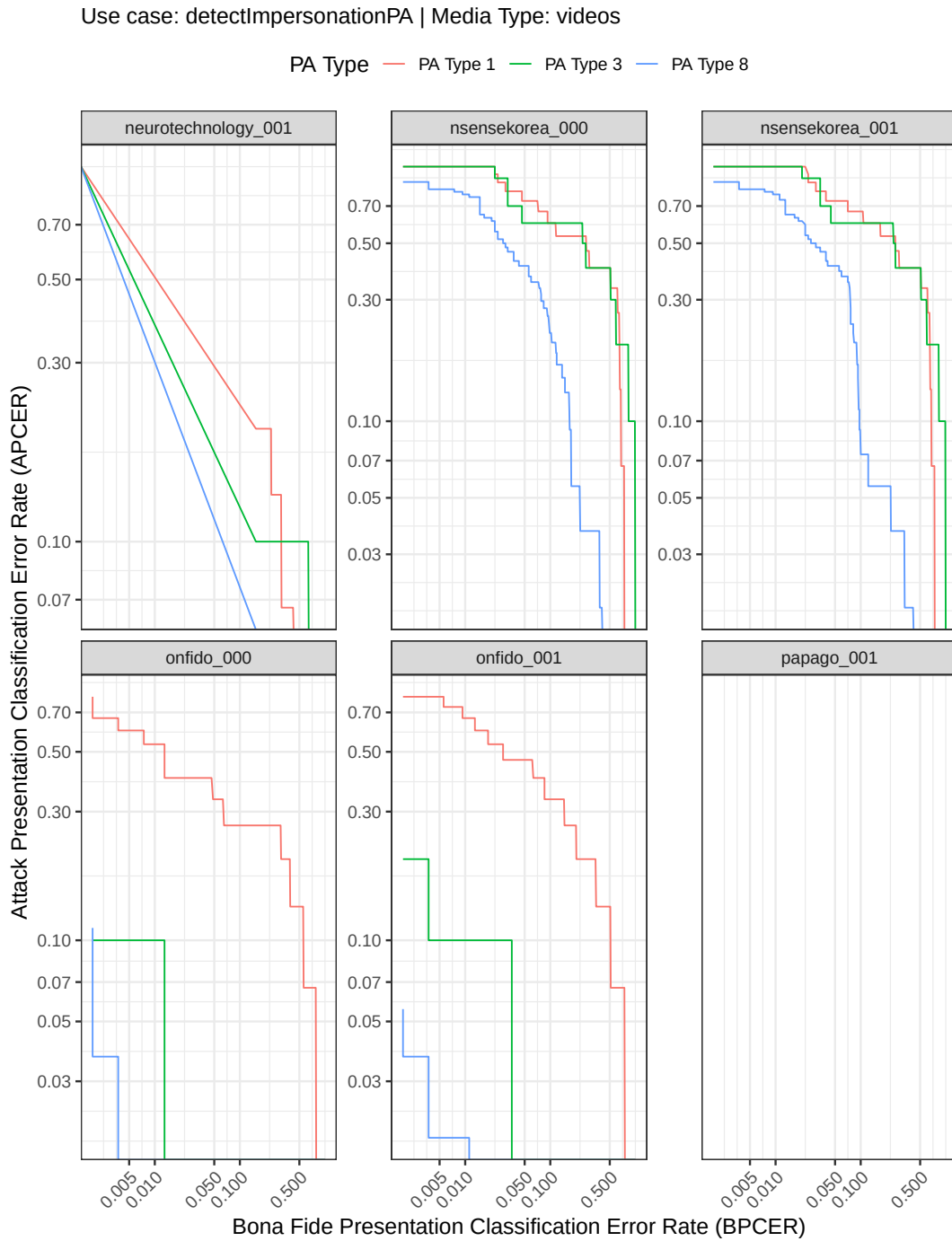


Fig. 35. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

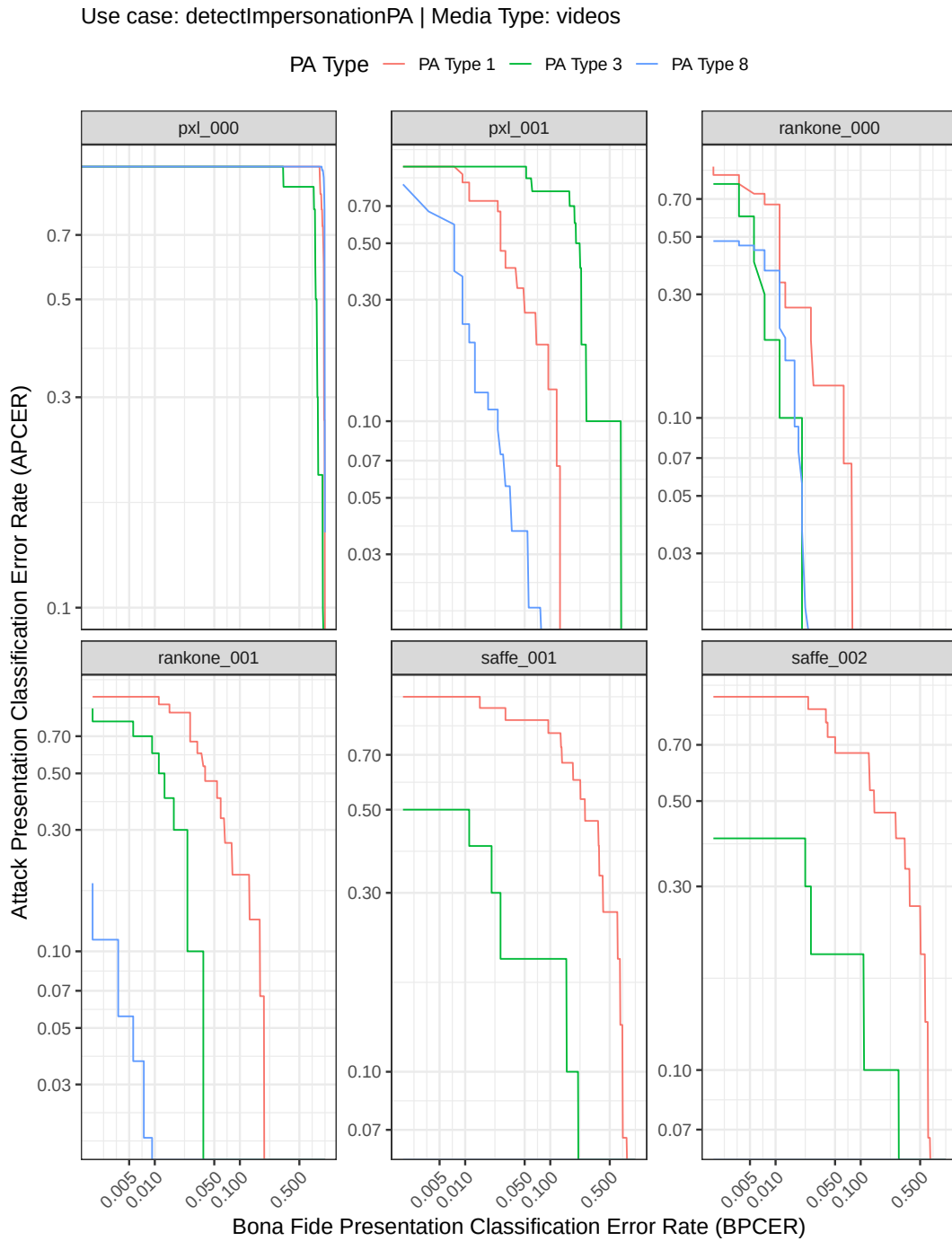


Fig. 36. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

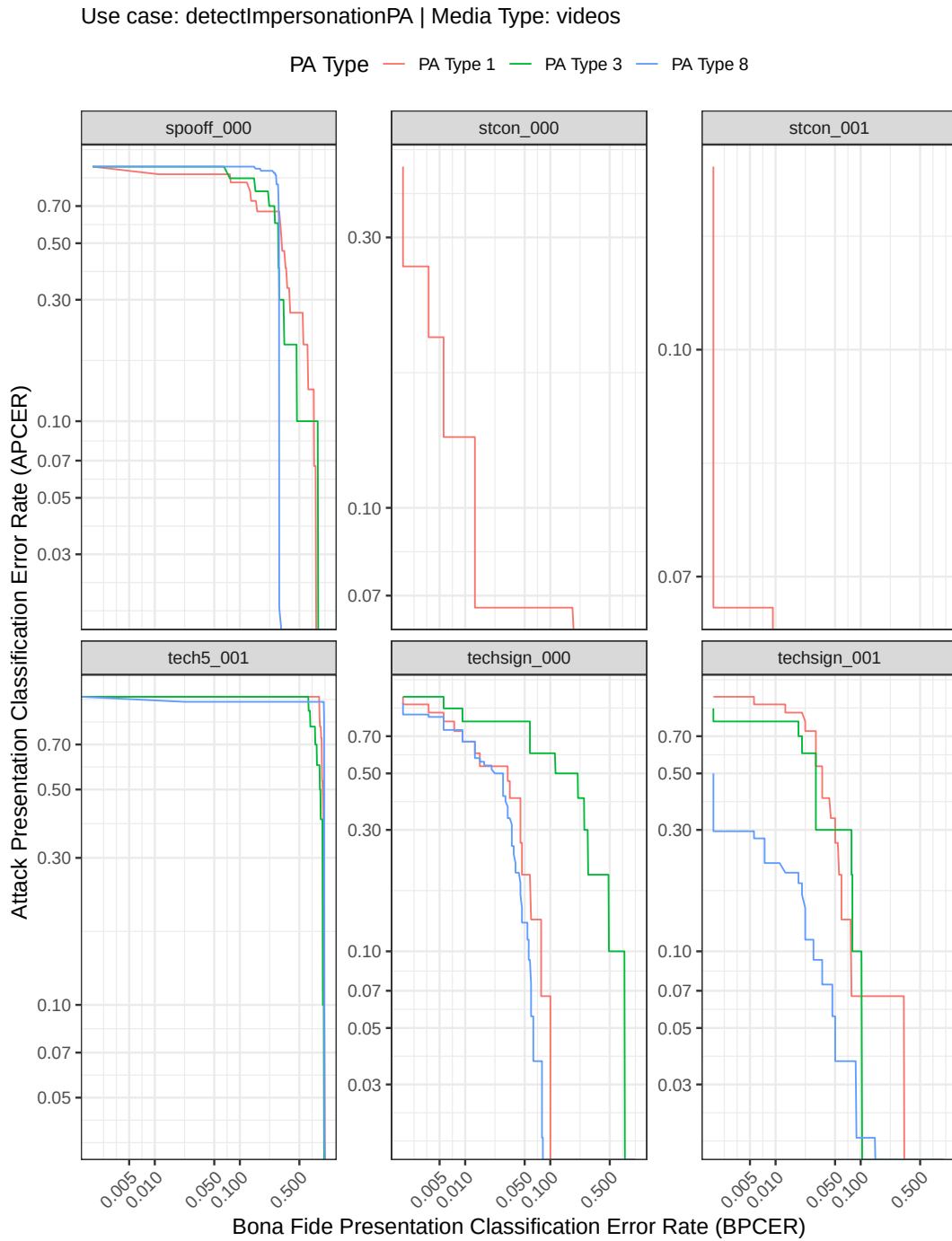


Fig. 37. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

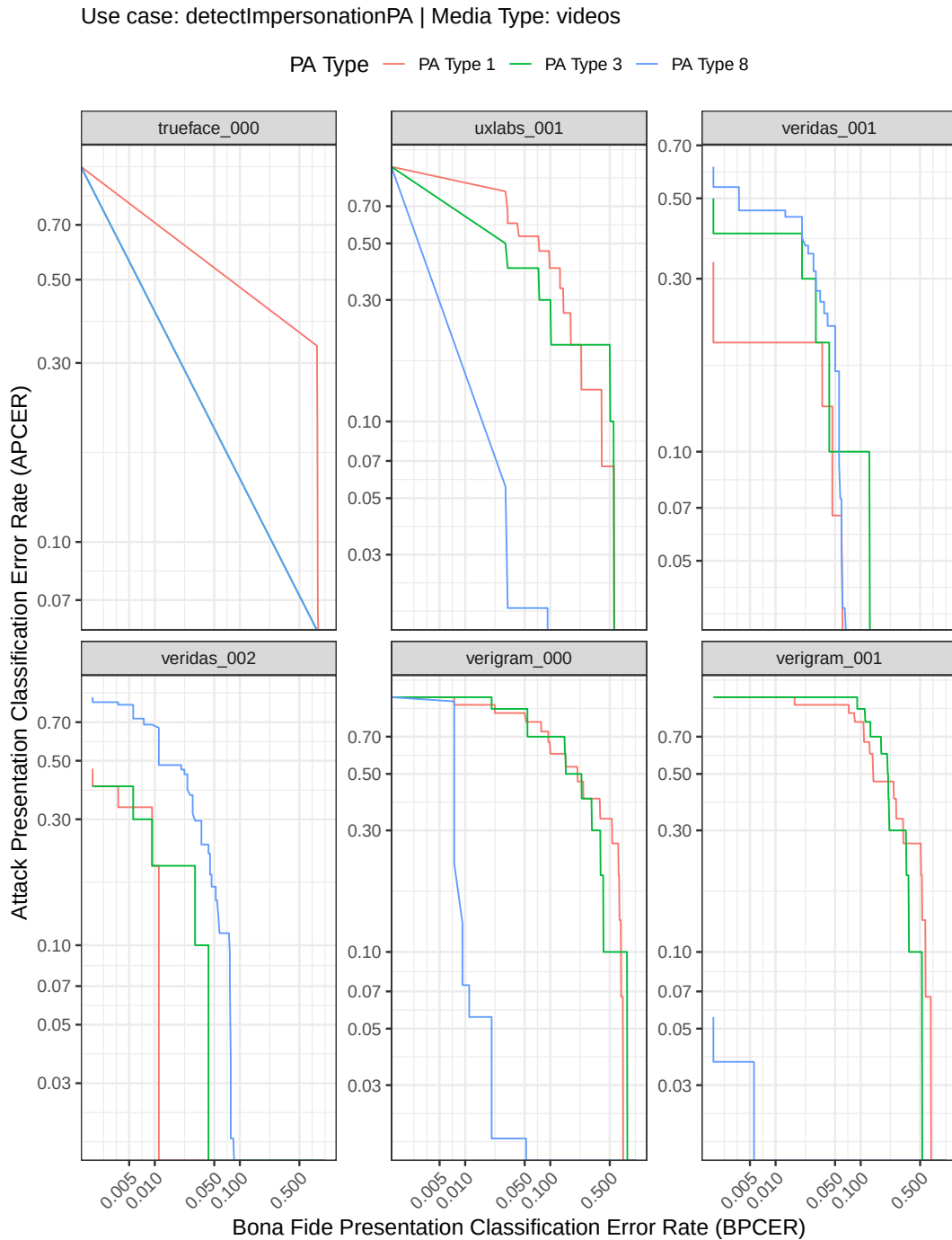


Fig. 38. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.

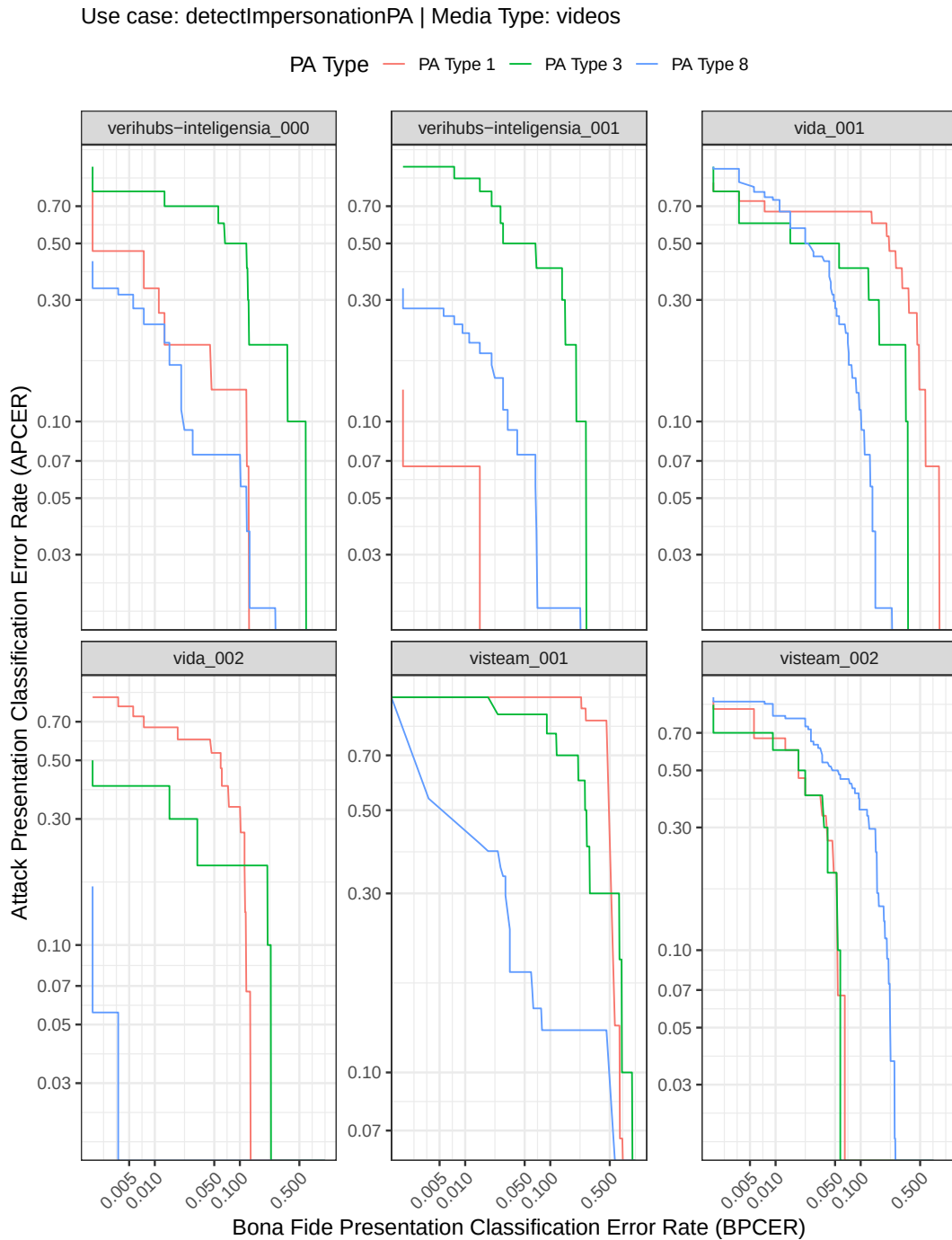
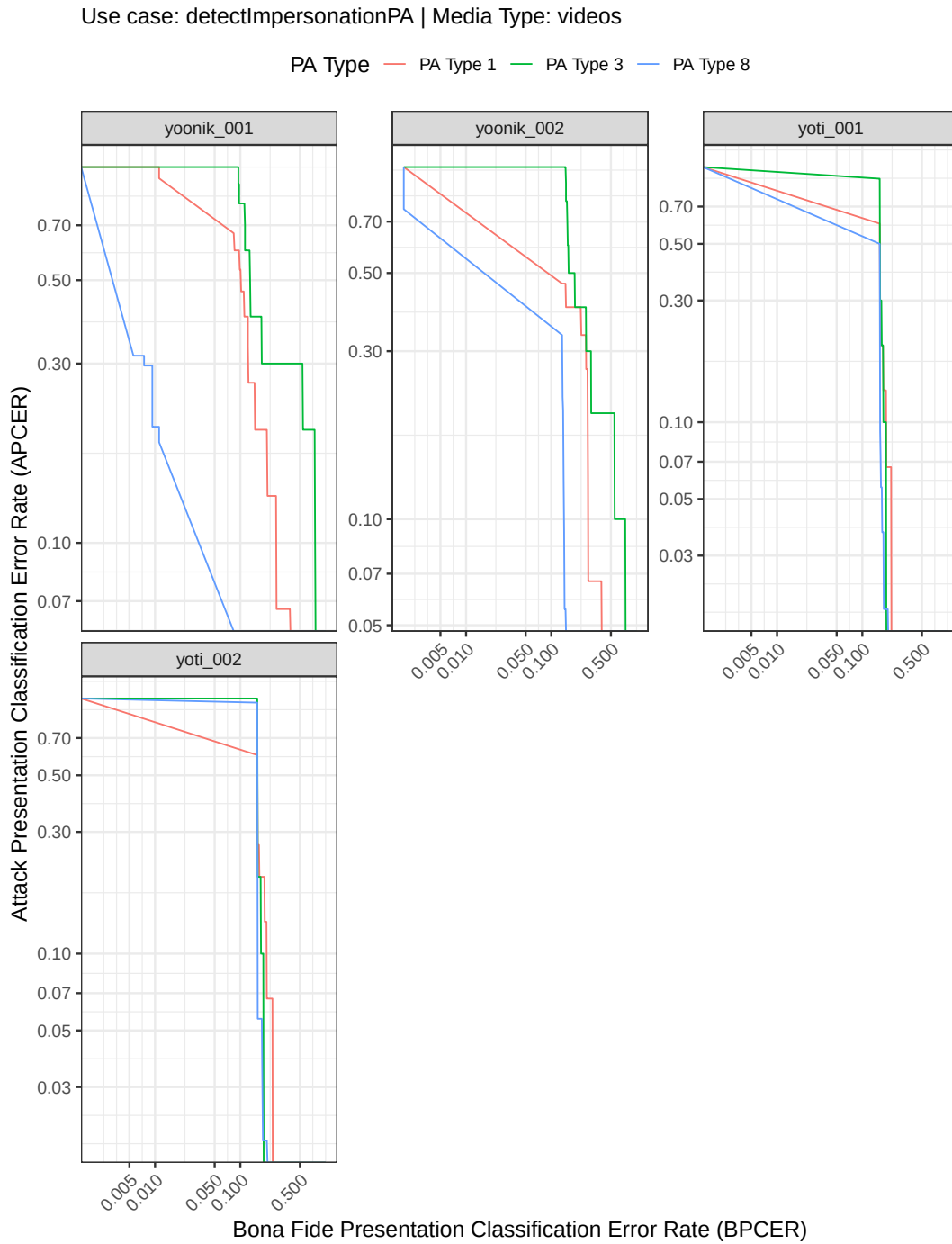


Fig. 39. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of impersonation PA videos.



Appendix A.3. Evasion

Table 39. PA Type 1 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
kakao-001	0.000	0.000	0.13 ± 0.01	1	0.151	1
kakao-000	0.000	0.000	0.28 ± 0.02	2	0.635	9
rankone-000	0.000	0.000	0.39 ± 0.02	3	0.665	10
rankone-001	0.000	0.000	0.39 ± 0.02	3	0.665	10
kasikornlabs-000	0.024	0.000	0.4 ± 0.02	5	0.495	4
cyberlink-002	0.000	0.000	0.44 ± 0.02	6	0.254	2
aware-002	0.000	0.000	0.51 ± 0.02	7	0.418	3
neurotechnology-000	0.000	0.000	0.53 ± 0.02	8	1.000	24
kasikornlabs-001	0.024	0.000	0.53 ± 0.02	9	0.542	7
onfido-000	0.049	0.000	0.55 ± 0.02	10	0.934	15
onfido-001	0.049	0.000	0.62 ± 0.02	11	0.696	12
facedirect-002	0.000	0.000	0.73 ± 0.02	12	1.000	24
trueface-000	0.000	0.000	0.75 ± 0.01	13	1.000	24
griaule-001	0.000	0.000	0.79 ± 0.01	14	0.989	19
griaule-000	0.000	0.000	0.86 ± 0.01	15	0.998	20
facedirect-001	0.000	0.000	0.88 ± 0.01	16	0.978	16
cyberlink-001	0.001	0.001	0.88 ± 0.01	17	0.696	12
cubox-000	0.003	0.000	0.928 ± 0.009	18	0.978	16
cubox-001	0.003	0.000	0.974 ± 0.006	19	1.000	21
spooff-000	0.000	0.000	0.976 ± 0.005	20	1.000	24
papago-001	0.000	0.000	0.989 ± 0.003	21	1.000	21
jcv-001	0.000	0.000	0.99 ± 0.003	22	0.989	18
alchera-000	0.000	0.000	1 ± 0.0005	23	1.000	21
alice-000	0.000	0.000	1 ± 0	24	0.517	6
aware-001	0.148	0.035	1 ± 0	24	0.507	5
neurotechnology-001	0.000	0.000	1 ± 0	24	0.863	14
uxlabs-001	0.000	0.000	1 ± 0	24	0.600	8

Table 40. PA Type 2 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kakao-001	0.000	0.000	0.12 ± 0.06	1	0.108	3
onfido-000	0.000	0.000	0.17 ± 0.07	2	0.221	6
kakao-000	0.000	0.000	0.18 ± 0.07	3	0.315	8
aware-002	0.000	0.000	0.33 ± 0.09	4	0.173	5
onfido-001	0.000	0.000	0.4 ± 0.1	5	0.463	12
neurotechnology-000	0.000	0.000	0.4 ± 0.1	6	0.297	7
cyberlink-002	0.000	0.000	0.4 ± 0.1	7	0.077	2
kasikornlabs-000	0.000	0.000	0.5 ± 0.1	8	0.437	11
kasikornlabs-001	0.000	0.000	0.6 ± 0.1	9	0.386	10
facedirect-002	0.000	0.000	0.64 ± 0.09	10	1.000	25
rankone-000	0.000	0.000	0.72 ± 0.09	11	0.643	13
rankone-001	0.000	0.000	0.72 ± 0.09	11	0.643	13
facedirect-001	0.000	0.000	0.83 ± 0.07	13	0.903	17
trueface-000	0.000	0.000	0.96 ± 0.03	14	1.000	25
griaule-000	0.000	0.000	0.98 ± 0.02	15	0.978	20
cubox-000	0.000	0.000	0.99 ± 0.01	16	0.989	21
cyberlink-001	0.000	0.001	0.99 ± 0.01	16	0.361	9
griaule-001	0.000	0.000	0.99 ± 0.01	16	0.924	18
alchera-000	0.000	0.000	1 ± 0	19	1.000	23
alice-000	0.000	0.000	1 ± 0	19	0.035	1
aware-001	0.105	0.035	1 ± 0	19	0.171	4
cubox-001	0.000	0.000	1 ± 0	19	0.967	19
jcv-001	0.000	0.000	1 ± 0	19	1.000	22
neurotechnology-001	0.000	0.000	1 ± 0	19	0.643	13
papago-001	0.000	0.000	1 ± 0	19	1.000	23
spoooff-000	0.000	0.000	1 ± 0	19	1.000	25
uxlabs-001	0.000	0.000	1 ± 0	19	0.711	16

Table 41. PA Type 3 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
onfido-000	0.000	0.000	0.05 ± 0.03	1	0.036	2
onfido-001	0.000	0.000	0.09 ± 0.04	2	0.051	4
aware-002	0.000	0.000	0.1 ± 0.04	3	0.057	6
facedirect-002	0.000	0.000	0.16 ± 0.05	4	0.989	23
neurotechnology-000	0.000	0.000	0.26 ± 0.06	5	0.197	7
kasikornlabs-000	0.000	0.000	0.26 ± 0.06	6	0.251	8
kasikornlabs-001	0.000	0.000	0.29 ± 0.06	7	0.329	10
kakao-001	0.000	0.000	0.56 ± 0.07	8	0.452	13
cyberlink-002	0.000	0.000	0.6 ± 0.07	9	0.041	3
kakao-000	0.000	0.000	0.68 ± 0.06	10	0.834	17
rankone-000	0.000	0.000	0.75 ± 0.06	11	0.753	15
rankone-001	0.000	0.000	0.75 ± 0.06	11	0.753	15
facedirect-001	0.000	0.000	0.83 ± 0.05	13	0.390	11
cubox-000	0.000	0.000	0.92 ± 0.04	14	0.967	19
cubox-001	0.000	0.000	0.95 ± 0.03	15	0.934	18
trueface-000	0.000	0.000	0.98 ± 0.02	16	1.000	26
jcv-001	0.000	0.000	0.99 ± 0.02	17	0.989	21
griaule-001	0.000	0.000	0.995 ± 0.007	18	1.000	24
papago-001	0.000	0.000	0.995 ± 0.007	18	0.989	22
alchera-000	0.000	0.000	1 ± 0	20	1.000	24
alice-000	0.000	0.000	1 ± 0	20	0.014	1
aware-001	0.072	0.035	1 ± 0	20	0.052	5
cyberlink-001	0.000	0.001	1 ± 0	20	0.574	14
griaule-000	0.000	0.000	1 ± 0	20	0.978	20
neurotechnology-001	0.000	0.000	1 ± 0	20	0.297	9
spoooff-000	0.000	0.000	1 ± 0	20	1.000	26
uxlabs-001	0.000	0.000	1 ± 0	20	0.447	12

Table 42. PA Type 4 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kasikornlabs-000	0.000	0.000	0.62 ± 0.04	1	0.452	4
kasikornlabs-001	0.000	0.000	0.62 ± 0.04	2	0.555	5
cyberlink-002	0.000	0.000	0.63 ± 0.04	3	0.446	3
onfido-001	0.000	0.000	0.74 ± 0.03	4	0.621	6
aware-002	0.000	0.000	0.76 ± 0.03	5	0.348	2
kakao-001	0.000	0.000	0.82 ± 0.03	6	0.815	9
onfido-000	0.000	0.000	0.82 ± 0.03	6	0.788	7
kakao-000	0.000	0.000	0.89 ± 0.03	8	0.912	11
facedirect-001	0.000	0.000	0.9 ± 0.02	9	0.989	19
cubox-001	0.000	0.000	0.9 ± 0.02	10	0.967	16
rankone-000	0.000	0.000	0.91 ± 0.02	11	0.913	12
rankone-001	0.000	0.000	0.91 ± 0.02	11	0.913	12
neurotechnology-000	0.000	0.000	0.91 ± 0.02	13	1.000	25
cubox-000	0.000	0.000	0.95 ± 0.02	14	0.967	16
cyberlink-001	0.000	0.001	0.98 ± 0.01	15	0.945	14
facedirect-002	0.000	0.000	0.98 ± 0.01	16	0.989	21
jcv-001	0.000	0.000	0.987 ± 0.009	17	0.989	18
papago-001	0.000	0.000	0.992 ± 0.007	18	0.989	19
alchera-000	0.000	0.000	0.997 ± 0.004	19	1.000	23
spooff-000	0.000	0.000	0.998 ± 0.002	20	1.000	25
alice-000	0.000	0.000	1 ± 0	21	0.813	8
aware-001	0.139	0.035	1 ± 0	21	0.191	1
griaule-000	0.000	0.000	1 ± 0	21	0.998	22
griaule-001	0.000	0.000	1 ± 0	21	1.000	23
neurotechnology-001	0.000	0.000	1 ± 0	21	0.883	10
trueface-000	0.000	0.000	1 ± 0	21	1.000	25
uxlabs-001	0.000	0.000	1 ± 0	21	0.964	15

Table 43. PA Type 5 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
kakao-001	0.000	0.000	0 ± 0	1	0.001	1
kakao-000	0.000	0.000	0.02 ± 0.01	2	0.034	2
cyberlink-002	0.000	0.000	0.34 ± 0.06	3	0.560	7
facedirect-002	0.000	0.000	0.44 ± 0.06	4	1.000	25
aware-002	0.000	0.000	0.65 ± 0.06	5	0.390	4
griaule-000	0.000	0.000	0.68 ± 0.06	6	0.966	18
rankone-000	0.000	0.000	0.73 ± 0.05	7	0.665	8
rankone-001	0.000	0.000	0.73 ± 0.05	7	0.665	8
onfido-001	0.000	0.000	0.79 ± 0.05	9	0.788	11
onfido-000	0.000	0.000	0.82 ± 0.04	10	0.844	12
griaule-001	0.000	0.000	0.85 ± 0.04	11	0.989	19
trueface-000	0.000	0.000	0.9 ± 0.04	12	1.000	25
neurotechnology-000	0.000	0.000	0.92 ± 0.03	13	1.000	25
kasikornlabs-000	0.000	0.000	0.96 ± 0.02	14	0.989	19
cyberlink-001	0.000	0.001	0.97 ± 0.02	15	0.873	14
kasikornlabs-001	0.000	0.000	0.97 ± 0.02	16	0.989	19
cubox-000	0.000	0.000	0.98 ± 0.01	17	0.934	17
cubox-001	0.000	0.000	0.99 ± 0.01	18	0.924	16
facedirect-001	0.000	0.000	0.99 ± 0.01	18	1.000	23
jcv-001	0.000	0.000	0.99 ± 0.01	20	1.000	22
spoooff-000	0.000	0.000	0.99 ± 0.01	20	0.497	6
alchera-000	0.000	0.000	1 ± 0	22	1.000	23
alice-000	0.000	0.000	1 ± 0	22	0.851	13
aware-001	0.004	0.035	1 ± 0	22	0.495	5
neurotechnology-001	0.000	0.000	1 ± 0	22	0.913	15
papago-001	0.000	0.000	1 ± 0	22	0.696	10
uxlabs-001	0.000	0.000	1 ± 0	22	0.207	3

Table 44. PA Type 6 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
rankone-000	0.000	0.000	0 ± 0	1	0.000	1
rankone-001	0.000	0.000	0 ± 0	1	0.000	1
trueface-000	0.000	0.000	0.002 ± 0.002	3	0.003	3
kakao-000	0.000	0.000	0.008 ± 0.005	4	0.004	4
cyberlink-002	0.000	0.000	0.012 ± 0.006	5	0.011	5
kakao-001	0.000	0.000	0.014 ± 0.007	6	0.012	6
neurotechnology-000	0.000	0.000	0.21 ± 0.02	7	0.226	13
griaule-001	0.000	0.000	0.34 ± 0.03	8	0.337	14
griaule-000	0.000	0.000	0.49 ± 0.03	9	0.447	15
aware-002	0.000	0.000	0.51 ± 0.03	10	0.053	8
kasikornlabs-000	0.028	0.000	0.69 ± 0.03	11	0.567	16
cyberlink-001	0.000	0.001	0.73 ± 0.02	12	0.119	9
facedirect-002	0.000	0.000	0.75 ± 0.02	13	1.000	26
kasikornlabs-001	0.028	0.000	0.8 ± 0.02	14	0.657	18
onfido-001	0.046	0.000	0.81 ± 0.02	15	0.587	17
facedirect-001	0.000	0.000	0.86 ± 0.02	16	0.967	20
onfido-000	0.046	0.000	0.9 ± 0.02	17	1.000	22
cubox-000	0.001	0.000	0.92 ± 0.02	18	0.934	19
spooff-000	0.000	0.000	0.94 ± 0.01	19	1.000	26
cubox-001	0.001	0.000	0.988 ± 0.006	20	1.000	22
papago-001	0.000	0.000	0.989 ± 0.006	21	1.000	22
jcv-001	0.000	0.000	0.99 ± 0.005	22	1.000	21
alchera-000	0.000	0.000	1 ± 0	23	1.000	22
alice-000	0.000	0.000	1 ± 0	23	0.138	11
aware-001	0.178	0.035	1 ± 0	23	0.038	7
neurotechnology-001	0.000	0.000	1 ± 0	23	0.224	12
uxlabs-001	0.000	0.000	1 ± 0	23	0.133	10

Table 45. PA Type 7 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kakao-001	0.000	0.000	0.14 ± 0.01	1	0.202	2
kakao-000	0.000	0.000	0.15 ± 0.01	2	0.574	8
onfido-001	0.001	0.000	0.34 ± 0.01	3	0.284	3
onfido-000	0.001	0.000	0.43 ± 0.01	4	0.779	14
rankone-000	0.000	0.000	0.52 ± 0.01	5	0.607	9
rankone-001	0.000	0.000	0.52 ± 0.01	5	0.607	9
cyberlink-002	0.000	0.000	0.52 ± 0.01	7	0.035	1
neurotechnology-000	0.000	0.000	0.65 ± 0.01	8	0.525	7
aware-002	0.000	0.000	0.8 ± 0.01	9	0.473	5
kasikornlabs-000	0.000	0.000	0.84 ± 0.01	10	0.728	12
kasikornlabs-001	0.000	0.000	0.86 ± 0.01	11	0.745	13
facedirect-002	0.000	0.000	0.86 ± 0.01	12	1.000	25
facedirect-001	0.000	0.000	0.86 ± 0.01	13	0.978	19
trueface-000	0.000	0.000	0.922 ± 0.008	14	1.000	25
cubox-001	0.000	0.000	0.949 ± 0.006	15	0.945	17
griaule-001	0.000	0.000	0.957 ± 0.006	16	0.967	18
griaule-000	0.000	0.000	0.96 ± 0.006	17	0.989	20
cyberlink-001	0.001	0.001	0.975 ± 0.004	18	0.893	16
cubox-000	0.000	0.000	0.98 ± 0.004	19	0.989	20
papago-001	0.000	0.000	0.987 ± 0.003	20	1.000	23
jcv-001	0.000	0.000	0.992 ± 0.002	21	1.000	22
spoooff-000	0.000	0.000	0.994 ± 0.002	22	1.000	25
alchera-000	0.000	0.000	1 ± 0.0003	23	1.000	23
alice-000	0.000	0.000	1 ± 0	24	0.377	4
aware-001	0.151	0.035	1 ± 0	24	0.657	11
neurotechnology-001	0.000	0.000	1 ± 0	24	0.806	15
uxlabs-001	0.000	0.000	1 ± 0	24	0.495	6

Table 46. PA Type 8 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
kakao-000	0.000	0.000	0.009 ± 0.005	1	0.006	1
onfido-001	0.000	0.000	0.017 ± 0.007	2	0.020	5
kakao-001	0.000	0.000	0.018 ± 0.007	3	0.013	2
onfido-000	0.000	0.000	0.024 ± 0.008	4	0.019	4
aware-002	0.000	0.000	0.08 ± 0.01	5	0.075	7
kasikornlabs-000	0.000	0.000	0.09 ± 0.01	6	0.126	9
neurotechnology-000	0.000	0.000	0.1 ± 0.02	7	0.095	8
kasikornlabs-001	0.000	0.000	0.15 ± 0.02	8	0.141	10
facedirect-002	0.000	0.000	0.47 ± 0.03	9	1.000	25
cyberlink-002	0.000	0.000	0.51 ± 0.03	10	0.067	6
facedirect-001	0.000	0.000	0.86 ± 0.02	11	0.967	16
cubox-001	0.000	0.000	0.88 ± 0.02	12	0.893	15
cubox-000	0.000	0.000	0.9 ± 0.02	13	0.806	14
trueface-000	0.000	0.000	0.972 ± 0.008	14	1.000	25
jcv-001	0.000	0.000	0.986 ± 0.006	15	0.989	20
griaule-000	0.000	0.000	0.989 ± 0.005	16	0.998	22
spooff-000	0.000	0.000	0.99 ± 0.005	17	1.000	25
cyberlink-001	0.004	0.001	0.991 ± 0.005	18	1.000	23
griaule-001	0.000	0.000	0.992 ± 0.005	19	0.989	21
rankone-000	0.000	0.000	0.996 ± 0.003	20	0.967	16
rankone-001	0.000	0.000	0.996 ± 0.003	20	0.967	16
alchera-000	0.000	0.000	1 ± 0	22	1.000	23
alice-000	0.000	0.000	1 ± 0	22	0.015	3
aware-001	0.114	0.035	1 ± 0	22	0.978	19
neurotechnology-001	0.000	0.000	1 ± 0	22	0.224	11
papago-001	0.000	0.000	1 ± 0	22	0.696	13
uxlabs-001	0.000	0.000	1 ± 0	22	0.678	12

Table 47. PA Type 8 (zoomed) - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
onfido-001	0.003	0.000	0.06 ± 0.01	1	0.096	2
onfido-000	0.003	0.000	0.07 ± 0.01	2	0.219	4
kakao-000	0.000	0.000	0.07 ± 0.01	3	0.099	3
kakao-001	0.000	0.000	0.12 ± 0.02	4	0.052	1
kasikornlabs-000	0.001	0.000	0.12 ± 0.02	5	0.574	7
kasikornlabs-001	0.001	0.000	0.22 ± 0.02	6	0.628	9
facedirect-002	0.000	0.000	0.3 ± 0.02	7	1.000	23
neurotechnology-000	0.000	0.000	0.3 ± 0.02	8	1.000	23
aware-002	0.000	0.000	0.31 ± 0.02	9	0.329	6
facedirect-001	0.000	0.000	0.83 ± 0.02	10	0.924	14
cubox-000	0.000	0.000	0.89 ± 0.02	11	0.806	11
cyberlink-002	0.000	0.000	0.9 ± 0.02	12	0.984	17
cubox-001	0.000	0.000	0.94 ± 0.01	13	0.893	13
spooff-000	0.000	0.000	0.96 ± 0.01	14	1.000	23
trueface-000	0.003	0.000	0.989 ± 0.005	15	1.000	23
jcv-001	0.000	0.000	0.99 ± 0.005	16	0.989	18
rankone-000	0.000	0.000	0.992 ± 0.005	17	0.967	15
rankone-001	0.000	0.000	0.992 ± 0.005	17	0.967	15
griaule-000	0.000	0.000	0.994 ± 0.004	19	0.998	21
griaule-001	0.000	0.000	0.994 ± 0.004	19	0.989	19
cyberlink-001	0.002	0.001	0.998 ± 0.002	21	1.000	22
papago-001	0.000	0.000	0.999 ± 0.002	22	0.696	10
alchera-000	0.000	0.000	1 ± 0	23	1.000	23
alice-000	0.000	0.000	1 ± 0	23	0.813	12
aware-001	0.117	0.035	1 ± 0	23	0.989	19
neurotechnology-001	0.000	0.000	1 ± 0	23	0.224	5
uxlabs-001	0.000	0.000	1 ± 0	23	0.628	8

Table 48. PA Type 9 - Use Case: detectEvasionPA - Media Type: stills

Algorithm	APNRR	BPNNR	(Convenience) APCER @ BPCER=0.01	Rank	(Security) BPCER @ APCER=0.01	Rank
kasikornlabs-000	0.005	0.000	0.052 ± 0.005	1	0.055	3
kasikornlabs-001	0.005	0.000	0.063 ± 0.006	2	0.095	5
onfido-000	0.006	0.000	0.068 ± 0.006	3	0.146	6
kakao-001	0.000	0.000	0.107 ± 0.007	4	0.242	10
onfido-001	0.006	0.000	0.135 ± 0.008	5	0.195	8
kakao-000	0.000	0.000	0.26 ± 0.01	6	0.761	16
rankone-000	0.000	0.000	0.27 ± 0.01	7	0.580	13
rankone-001	0.000	0.000	0.27 ± 0.01	7	0.580	13
aware-002	0.000	0.000	0.34 ± 0.01	9	0.161	7
cyberlink-002	0.000	0.000	0.41 ± 0.01	10	0.027	1
facedirect-002	0.000	0.000	0.44 ± 0.01	11	1.000	25
neurotechnology-000	0.001	0.000	0.53 ± 0.01	12	0.442	12
facedirect-001	0.000	0.000	0.836 ± 0.009	13	0.913	17
cubox-000	0.000	0.000	0.907 ± 0.007	14	0.967	19
cyberlink-001	0.001	0.001	0.907 ± 0.007	15	0.322	11
trueface-000	0.000	0.000	0.947 ± 0.006	16	1.000	25
griaule-000	0.000	0.000	0.953 ± 0.005	17	0.978	20
griaule-001	0.000	0.000	0.972 ± 0.004	18	0.945	18
cubox-001	0.000	0.000	0.974 ± 0.004	19	1.000	22
papago-001	0.000	0.000	0.988 ± 0.003	20	1.000	22
jcv-001	0.000	0.000	0.99 ± 0.002	21	1.000	21
spooff-000	0.000	0.000	0.993 ± 0.002	22	1.000	25
alchera-000	0.000	0.000	0.998 ± 0.001	23	1.000	22
alice-000	0.000	0.000	1 ± 0	24	0.034	2
aware-001	0.096	0.035	1 ± 0	24	0.066	4
neurotechnology-001	0.000	0.000	1 ± 0	24	0.657	15
uxlabs-001	0.000	0.000	1 ± 0	24	0.200	9

Table 49. PA Type 1 - Use Case: detectEvasionPA - Media Type: videos

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kakao-001	0	0.000	0.14 ± 0.09	1	0.072	2
kasikornlabs-000	0	0.000	0.3 ± 0.1	2	0.418	4
kakao-000	0	0.000	0.3 ± 0.1	2	0.255	3
cyberlink-002	0	0.000	0.4 ± 0.1	4	0.050	1
kasikornlabs-001	0	0.000	0.4 ± 0.1	4	0.468	6
onfido-000	0	0.000	0.6 ± 0.1	6	0.853	13
neurotechnology-000	0	0.000	0.6 ± 0.1	6	0.535	7
onfido-001	0	0.000	0.7 ± 0.1	8	0.805	12
aware-001	0	0.002	0.7 ± 0.1	8	0.636	9
rankone-000	0	0.000	0.8 ± 0.1	10	0.924	17
rankone-001	0	0.000	0.8 ± 0.1	10	0.924	17
facedirect-001	0	0.000	0.91 ± 0.07	12	0.913	15
aware-002	0	0.000	0.91 ± 0.08	13	0.743	10
cubox-000	0	0.000	0.93 ± 0.06	14	0.853	13
cyberlink-001	0	0.000	0.93 ± 0.06	14	0.779	11
facedirect-002	0	0.000	0.96 ± 0.04	16	1.000	23
jcv-001	0	0.000	0.98 ± 0.03	17	0.998	22
trueface-000	0	0.000	0.98 ± 0.03	17	1.000	23
alchera-000	0	0.000	1 ± 0	19	1.000	23
alice-000	0	0.000	1 ± 0	19	0.463	5
cubox-001	0	0.000	1 ± 0	19	0.944	19
griaule-000	0	0.000	1 ± 0	19	0.976	20
griaule-001	0	0.000	1 ± 0	19	0.987	21
neurotechnology-001	0	0.000	1 ± 0	19	0.913	15
papago-001	0	0.000	1 ± 0	19	1.000	23
spoooff-000	0	0.000	1 ± 0	19	1.000	23
uxlabs-001	0	0.000	1 ± 0	19	0.567	8

Table 50. PA Type 3 - Use Case: detectEvasionPA - Media Type: videos

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
cyberlink-002	0	0.000	0 ± 0	1	0.006	1
kasikornlabs-000	0	0.000	0.1 ± 0.2	2	0.013	2
kasikornlabs-001	0	0.000	0.1 ± 0.2	2	0.059	9
onfido-000	0	0.000	0.1 ± 0.2	2	0.013	2
onfido-001	0	0.000	0.1 ± 0.2	2	0.035	5
aware-001	0	0.002	0.2 ± 0.2	6	0.024	4
aware-002	0	0.000	0.4 ± 0.3	7	0.080	11
kakao-001	0	0.000	0.4 ± 0.3	7	0.035	5
neurotechnology-000	0	0.000	0.4 ± 0.3	7	0.139	12
kakao-000	0	0.000	0.5 ± 0.3	10	0.050	8
facedirect-001	0	0.000	0.8 ± 0.2	11	0.046	7
rankone-000	0	0.000	0.9 ± 0.2	12	0.779	17
rankone-001	0	0.000	0.9 ± 0.2	12	0.779	17
alchera-000	0	0.000	1 ± 0	14	0.998	23
alice-000	0	0.000	1 ± 0	14	0.063	10
cubox-000	0	0.000	1 ± 0	14	0.976	20
cubox-001	0	0.000	1 ± 0	14	0.998	23
cyberlink-001	0	0.000	1 ± 0	14	0.230	13
facedirect-002	0	0.000	1 ± 0	14	0.991	22
griaule-000	0	0.000	1 ± 0	14	0.636	16
griaule-001	0	0.000	1 ± 0	14	0.987	21
jcv-001	0	0.000	1 ± 0	14	0.942	19
neurotechnology-001	0	0.000	1 ± 0	14	0.554	14
papago-001	0	0.000	1 ± 0	14	1.000	25
spooff-000	0	0.000	1 ± 0	14	1.000	25
trueface-000	0	0.000	1 ± 0	14	1.000	25
uxlabs-001	0	0.000	1 ± 0	14	0.561	15

Table 51. PA Type 5 - Use Case: detectEvasionPA - Media Type: videos

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kakao-001	0.00	0.000	0 ± 0	1	0.002	1
kakao-000	0.00	0.000	0.02 ± 0.03	2	0.011	2
facedirect-002	0.00	0.000	0.4 ± 0.1	3	1.000	23
griaule-000	0.00	0.000	0.5 ± 0.1	4	0.987	18
griaule-001	0.00	0.000	0.6 ± 0.1	5	0.944	16
cyberlink-002	0.00	0.000	0.7 ± 0.1	6	0.621	5
cyberlink-001	0.00	0.000	0.8 ± 0.1	7	0.872	13
aware-002	0.00	0.000	0.8 ± 0.1	7	0.665	6
onfido-000	0.00	0.000	0.8 ± 0.1	7	0.844	10
neurotechnology-000	0.00	0.000	0.88 ± 0.09	10	0.883	14
onfido-001	0.00	0.000	0.9 ± 0.09	11	0.712	8
trueface-000	0.00	0.000	0.92 ± 0.07	12	1.000	23
aware-001	0.02	0.002	0.96 ± 0.05	13	0.113	4
cubox-001	0.00	0.000	0.96 ± 0.05	13	0.987	18
kasikornlabs-000	0.00	0.000	0.96 ± 0.05	13	0.998	20
kasikornlabs-001	0.00	0.000	0.96 ± 0.05	13	0.998	20
cubox-000	0.00	0.000	0.98 ± 0.03	17	0.976	17
rankone-000	0.00	0.000	0.98 ± 0.03	17	0.853	11
rankone-001	0.00	0.000	0.98 ± 0.03	17	0.853	11
spooff-000	0.00	0.000	0.98 ± 0.03	17	0.779	9
alchera-000	0.00	0.000	1 ± 0	21	1.000	23
alice-000	0.00	0.000	1 ± 0	21	0.688	7
facedirect-001	0.00	0.000	1 ± 0	21	0.998	20
jcv-001	0.00	0.000	1 ± 0	21	1.000	23
neurotechnology-001	0.00	0.000	1 ± 0	21	0.892	15
papago-001	0.00	0.000	1 ± 0	21	1.000	23
uxlabs-001	0.00	0.000	1 ± 0	21	0.063	3

Table 52. PA Type 8 - Use Case: detectEvasionPA - Media Type: videos

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kasikornlabs-000	0	0.000	0 ± 0	1	0.002	1
kasikornlabs-001	0	0.000	0 ± 0	1	0.002	1
neurotechnology-000	0	0.000	0 ± 0	1	0.002	1
onfido-000	0	0.000	0 ± 0	1	0.004	4
onfido-001	0	0.000	0.02 ± 0.03	5	0.011	5
kakao-001	0	0.000	0.09 ± 0.07	6	0.087	8
kakao-000	0	0.000	0.11 ± 0.08	7	0.177	12
cyberlink-002	0	0.000	0.4 ± 0.1	8	0.022	6
facedirect-002	0	0.000	0.6 ± 0.1	9	0.991	22
facedirect-001	0	0.000	0.8 ± 0.1	10	0.987	21
aware-002	0	0.000	0.8 ± 0.1	10	0.370	13
cubox-001	0	0.000	0.96 ± 0.05	12	0.385	14
trueface-000	0	0.000	0.98 ± 0.03	13	1.000	23
alchera-000	0	0.000	1 ± 0	14	1.000	23
alice-000	0	0.000	1 ± 0	14	0.065	7
aware-001	0	0.002	1 ± 0	14	0.600	15
cubox-000	0	0.000	1 ± 0	14	0.095	10
cyberlink-001	0	0.000	1 ± 0	14	0.872	17
griaule-000	0	0.000	1 ± 0	14	1.000	23
griaule-001	0	0.000	1 ± 0	14	0.797	16
jcv-001	0	0.000	1 ± 0	14	0.985	20
neurotechnology-001	0	0.000	1 ± 0	14	0.154	11
papago-001	0	0.000	1 ± 0	14	1.000	23
rankone-000	0	0.000	1 ± 0	14	0.944	18
rankone-001	0	0.000	1 ± 0	14	0.944	18
spoooff-000	0	0.000	1 ± 0	14	1.000	23
uxlabs-001	0	0.000	1 ± 0	14	0.093	9

Table 53. PA Type 9 - Use Case: detectEvasionPA - Media Type: videos

Algorithm	APNRR	BPNRR	(Convenience)	Rank	(Security)	Rank
			APCER @ BPCER=0.01		BPCER @ APCER=0.01	
kasikornlabs-000	0.000	0.000	0 ± 0	1	0.002	1
kasikornlabs-001	0.000	0.000	0 ± 0	1	0.002	1
kakao-001	0.000	0.000	0.05 ± 0.07	3	0.015	3
onfido-000	0.000	0.000	0.1 ± 0.1	4	0.301	11
neurotechnology-000	0.000	0.000	0.2 ± 0.1	5	0.084	7
kakao-000	0.000	0.000	0.3 ± 0.1	6	0.309	12
onfido-001	0.000	0.000	0.4 ± 0.2	7	0.428	15
cyberlink-001	0.000	0.000	0.6 ± 0.2	8	0.136	9
aware-001	0.053	0.002	0.7 ± 0.1	9	0.041	4
rankone-000	0.000	0.000	0.7 ± 0.1	9	0.403	13
rankone-001	0.000	0.000	0.7 ± 0.1	9	0.403	13
cubox-001	0.000	0.000	0.8 ± 0.1	12	0.812	19
cyberlink-002	0.000	0.000	0.8 ± 0.1	12	0.052	5
aware-002	0.000	0.000	0.8 ± 0.1	12	0.719	18
facedirect-001	0.000	0.000	0.8 ± 0.1	12	0.480	16
facedirect-002	0.000	0.000	0.8 ± 0.1	12	0.991	22
cubox-000	0.000	0.000	0.9 ± 0.1	17	0.862	20
trueface-000	0.000	0.000	0.95 ± 0.07	18	1.000	25
alchera-000	0.000	0.000	1 ± 0	19	0.998	23
alice-000	0.000	0.000	1 ± 0	19	0.071	6
griaule-000	0.000	0.000	1 ± 0	19	0.955	21
griaule-001	0.000	0.000	1 ± 0	19	0.665	17
jcv-001	0.000	0.000	1 ± 0	19	0.998	23
neurotechnology-001	0.000	0.000	1 ± 0	19	0.234	10
papago-001	0.000	0.000	1 ± 0	19	1.000	25
spoooff-000	0.000	0.000	1 ± 0	19	1.000	25
uxlabs-001	0.000	0.000	1 ± 0	19	0.126	8

Fig. 40. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of evasion PA stills.

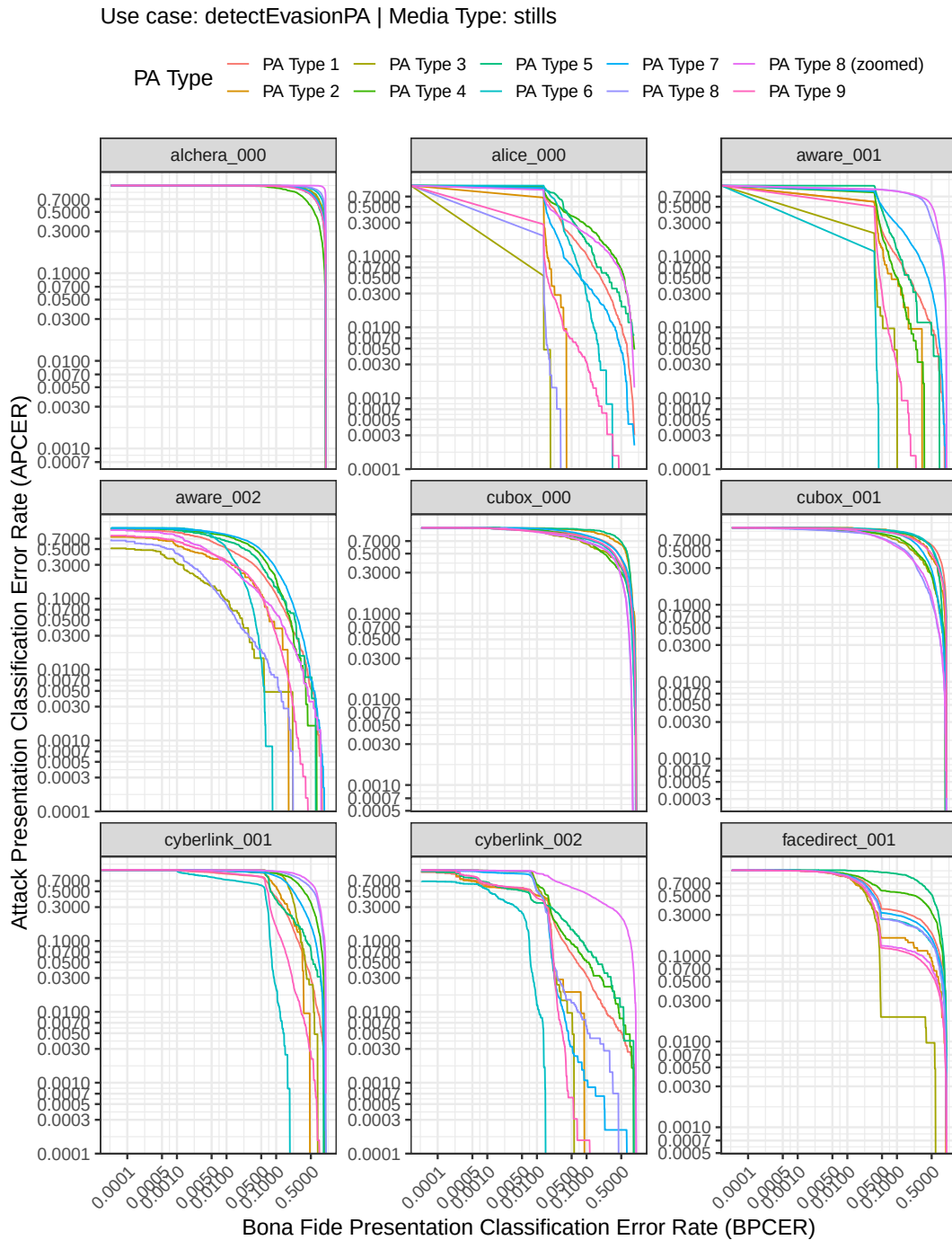


Fig. 41. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of evasion PA stills.

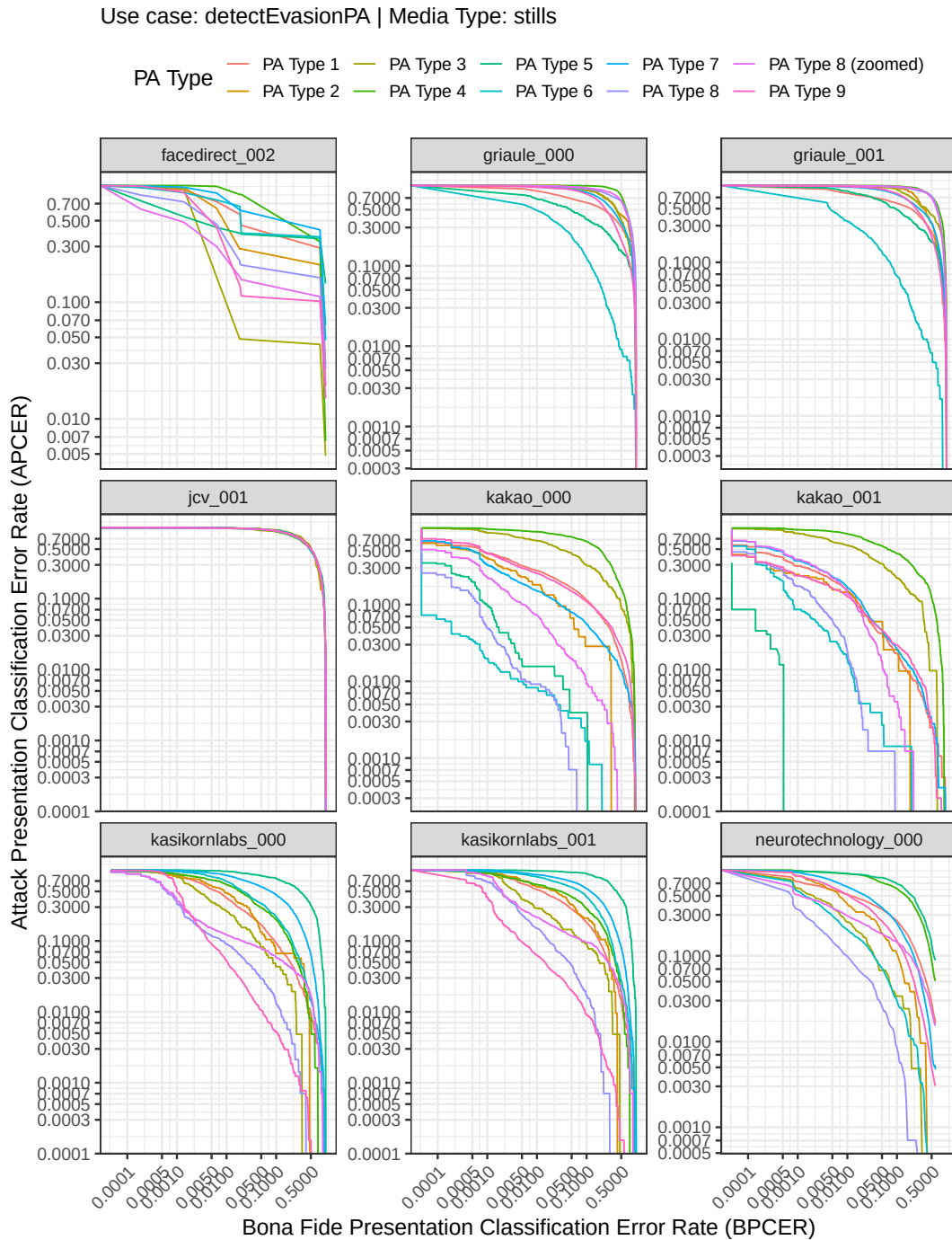


Fig. 42. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of evasion PA stills.

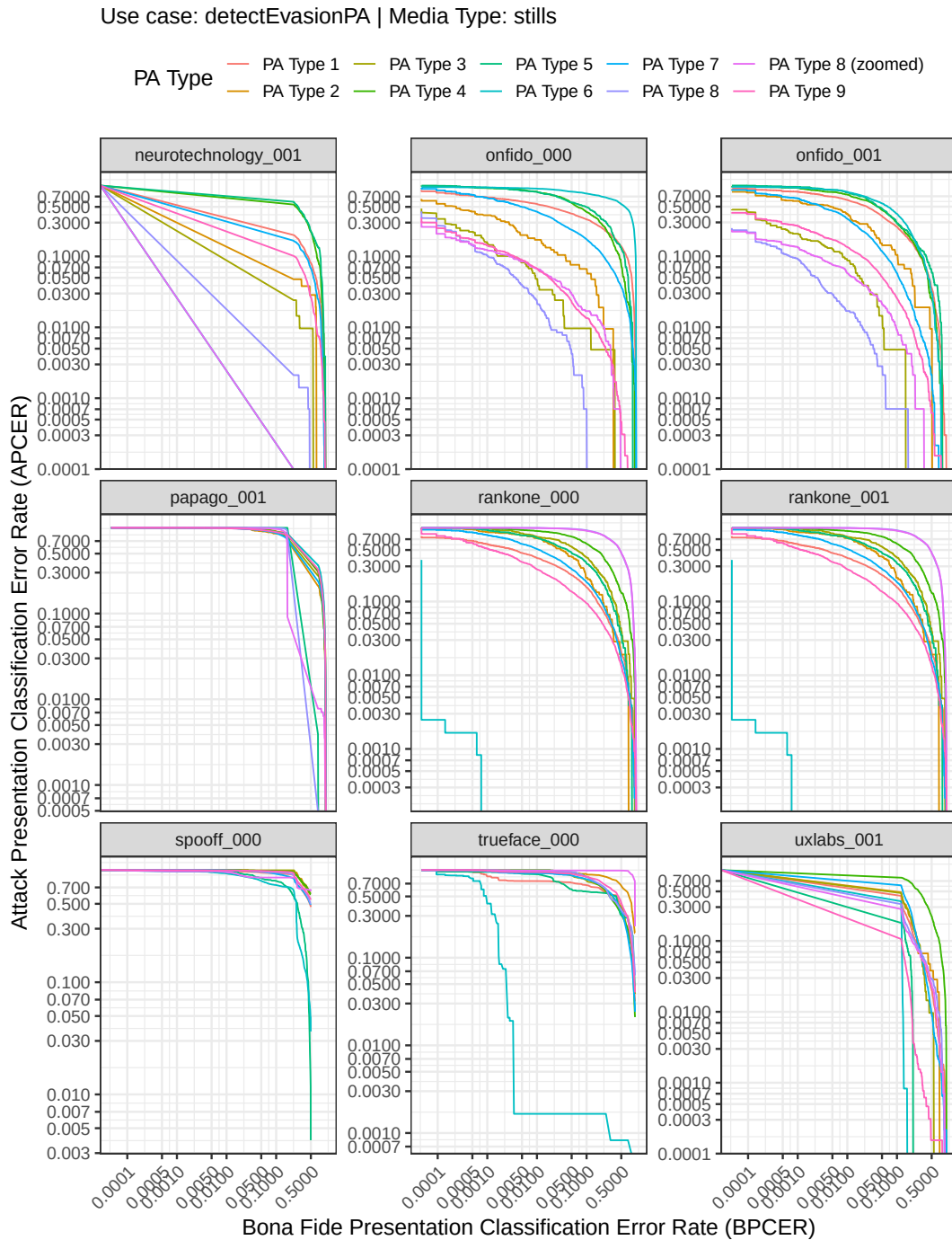


Fig. 43. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of evasion PA videos.

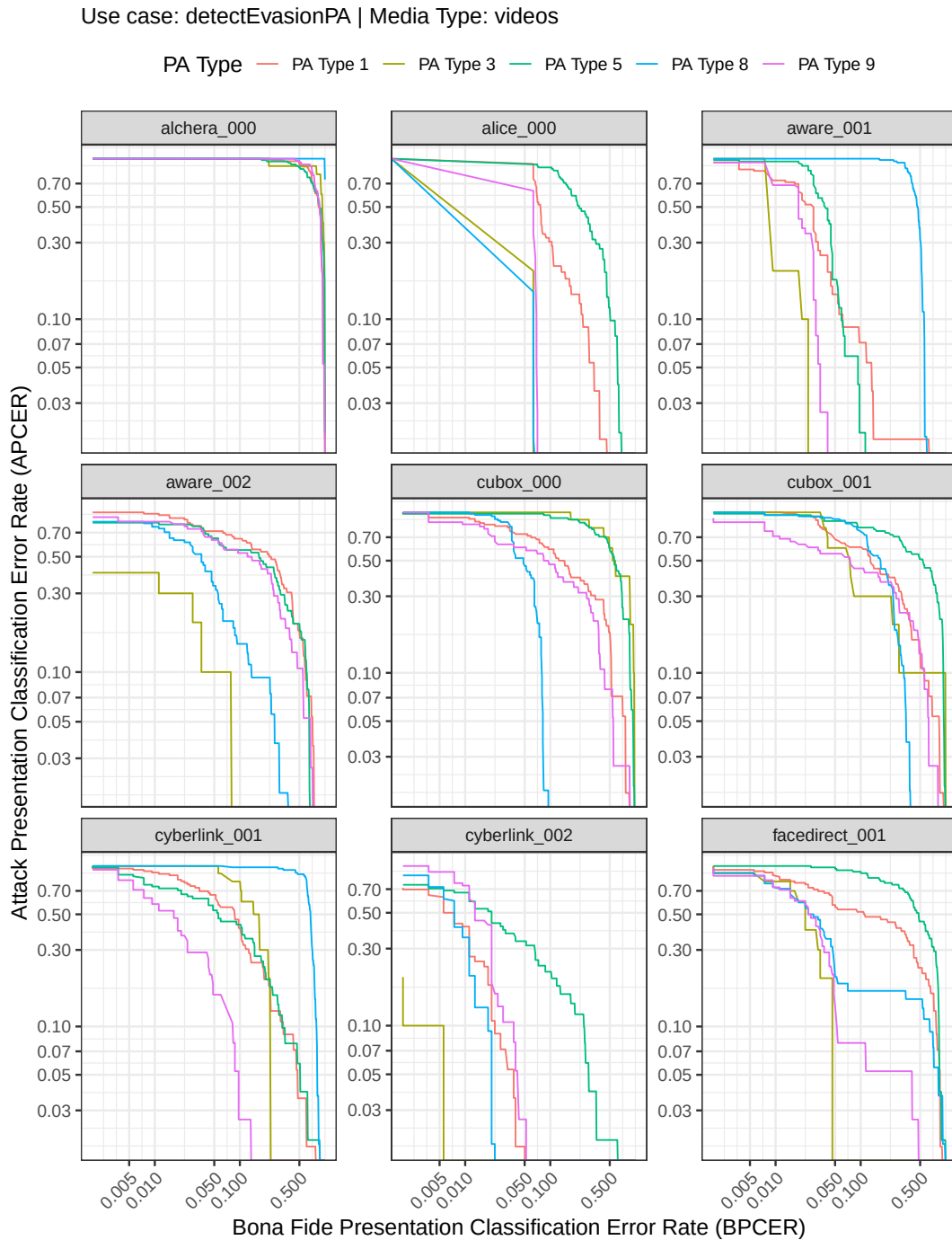


Fig. 44. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of evasion PA videos.

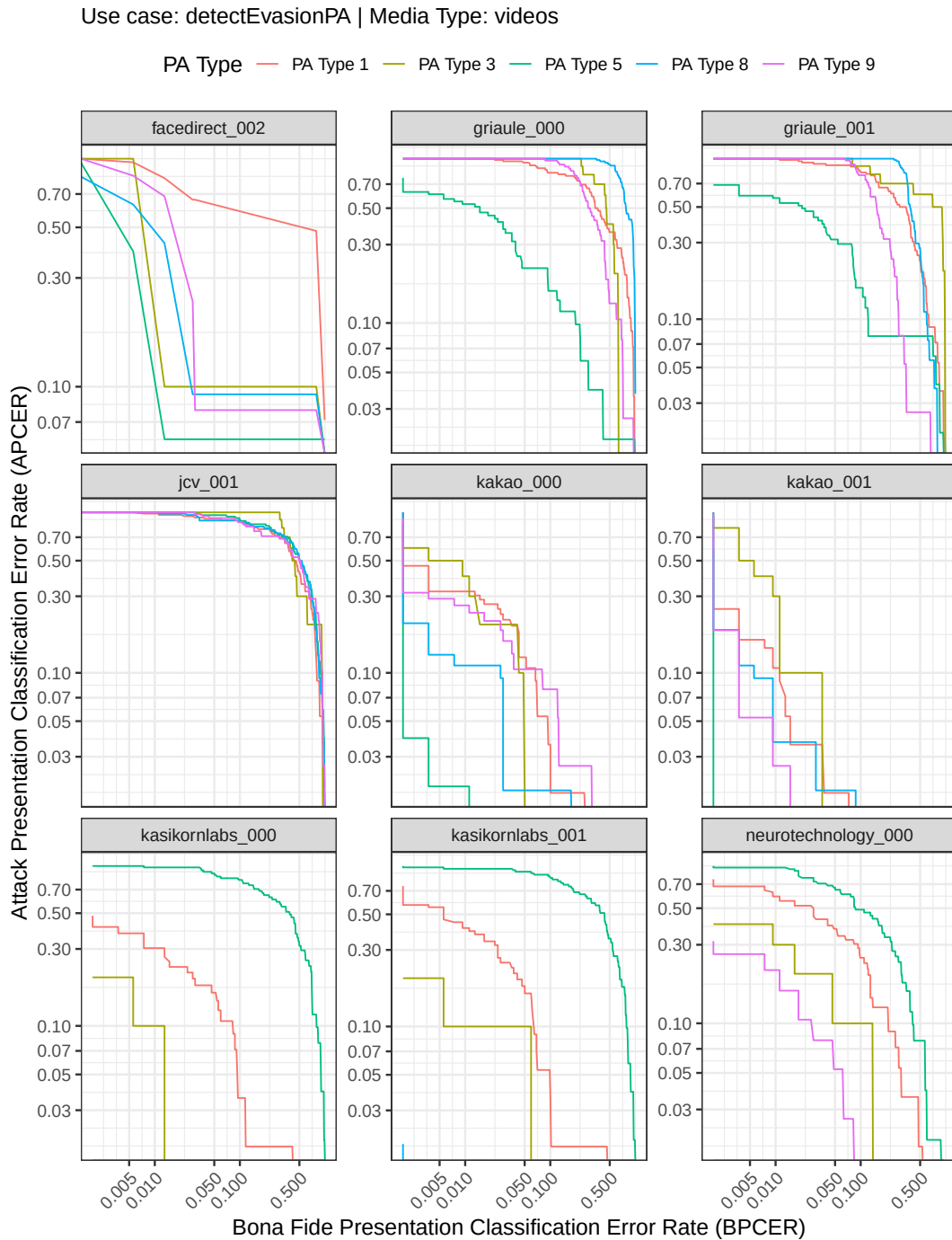
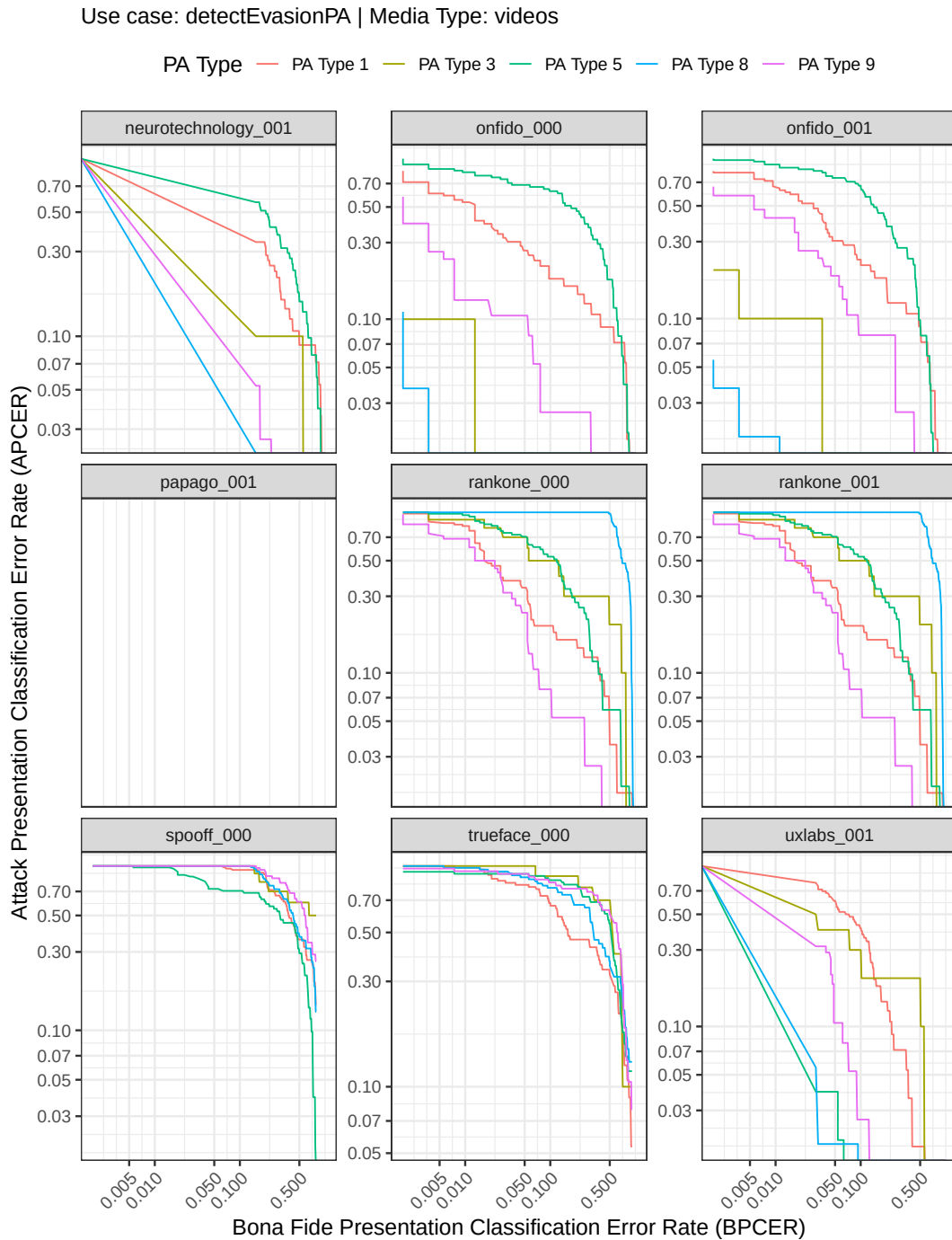


Fig. 45. This plot presents detection error tradeoff (DET) curves for PAD performance across different types of evasion PA videos.



Appendix B. Stills vs. Videos

Appendix B.1. Impersonation

Table 54. Use Case: detectImpersonationPA - Stills vs. Videos

Algorithm	(Convenience) APCER @ BPCER=0.01		Algorithm	(Security) BPCER @ APCER=0.01	
	Stills	Videos		Stills	Videos
alchera-000	1.00	1.00	alchera-000	1.00	1.00
alice-000	0.12	1.00	alice-000	0.20	0.18
alice-001	0.12	0.06	alice-001	0.53	0.46
aware-001	0.49	1.00	aware-001	0.20	0.14
aware-002	0.50	0.75	aware-002	0.29	0.60
biocube-001	0.94	0.82	biocube-001	0.89	0.80
biocube-002	0.92	0.82	biocube-002	0.76	0.90
cubox-000	0.94	0.96	cubox-000	0.99	0.98
cubox-001	1.00	0.97	cubox-001	0.91	1.00
cyberlink-001	0.03	0.03	cyberlink-001	0.03	0.03
cyberlink-002	0.00	0.00	cyberlink-002	0.00	0.01
facedirect-001	0.53	0.71	facedirect-001	0.99	0.99
facedirect-002	0.97	0.75	facedirect-002	1.00	0.99
facephi-000	1.00	0.11	facephi-000	0.28	0.26
facephi-001	1.00	0.19	facephi-001	0.59	0.66
griaule-000	0.23	0.25	griaule-000	0.68	0.67
griaule-001	0.40	0.63	griaule-001	1.00	0.21
hyperverge-001	0.13	0.11	hyperverge-001	0.31	0.15
hyperverge-002	0.14	0.18	hyperverge-002	1.00	0.07
id3-001	0.38	0.34	id3-001	0.92	0.88
idemia-010	0.50	0.30	idemia-010	0.26	0.18
idemia-011	0.23	0.20	idemia-011	0.80	0.88
idrnd-000	0.08	0.04	idrnd-000	0.08	0.09
idrnd-001	0.05	0.03	idrnd-001	0.07	0.03
idvisioncenter-001	0.59	0.25	idvisioncenter-001	0.82	0.90
idvisioncenter-002	0.82	0.59	idvisioncenter-002	0.77	0.69
iidentifi-000	0.09	0.08	iidentifi-000	0.24	0.17
incode-000	0.31	0.32	incode-000	0.49	0.31
incode-001	0.18	0.19	incode-001	1.00	0.28
innovatrics-001	0.24	0.19	innovatrics-001	0.92	0.68
innovatrics-002	0.47	0.18	innovatrics-002	0.64	0.61
intema-000	0.27	0.23	intema-000	0.85	0.64

intema-001	0.22	0.20	intema-001	0.81	0.62
iproov-000	0.05	1.00	iproov-000	0.05	0.03
iproov-001	0.05	0.03	iproov-001	0.05	0.07
jcv-001	0.19	1.00	jcv-001	0.84	1.00
jcv-002	0.22	1.00	jcv-002	1.00	0.73
kakao-000	0.15	0.14	kakao-000	0.14	0.16
kakao-001	0.01	0.04	kakao-001	0.07	0.05
kasikornlabs-000	0.10	0.04	kasikornlabs-000	0.19	0.02
kasikornlabs-001	0.27	0.06	kasikornlabs-001	0.25	0.06
mbsolutions-000	0.27	0.25	mbsolutions-000	1.00	0.87
mbsolutions-001	0.26	0.23	mbsolutions-001	1.00	0.87
meituan-000	0.26	0.15	meituan-000	0.88	0.80
meituan-001	0.24	0.23	meituan-001	1.00	0.19
mobbl-000	1.00	0.92	mobbl-000	0.83	0.91
mobbl-001	1.00	0.97	mobbl-001	1.00	0.81
neurotechnology-000	0.05	0.13	neurotechnology-000	0.36	0.14
neurotechnology-001	1.00	1.00	neurotechnology-001	0.76	0.64
nsensekorea-000	0.45	0.86	nsensekorea-000	0.87	1.00
nsensekorea-001	0.45	0.86	nsensekorea-001	0.87	1.00
onfido-000	0.06	0.11	onfido-000	0.35	0.79
onfido-001	0.14	0.15	onfido-001	0.60	0.75
papago-001	1.00	1.00	papago-001	1.00	1.00
pxl-000	1.00	1.00	pxl-000	1.00	1.00
pxl-001	0.65	0.46	pxl-001	0.40	0.68
rankone-000	0.42	0.41	rankone-000	0.23	0.08
rankone-001	0.23	0.29	rankone-001	0.27	0.20
saffe-001	0.24	0.25	saffe-001	0.80	0.79
saffe-002	0.23	0.23	saffe-002	0.78	0.65
spooff-000	0.95	1.00	spooff-000	0.86	0.83
stcon-000	0.09	0.03	stcon-000	0.55	0.19
stcon-001	0.03	0.01	stcon-001	0.05	0.01
tech5-001	1.00	1.00	tech5-001	1.00	1.00
techsign-000	0.97	0.76	techsign-000	0.93	0.76
techsign-001	0.71	0.43	techsign-001	0.71	0.33
trueface-000	1.00	1.00	trueface-000	0.65	0.83
uxlabs-001	1.00	1.00	uxlabs-001	0.53	0.57
veridas-001	0.44	0.41	veridas-001	0.21	0.13
veridas-002	0.50	0.52	veridas-002	0.28	0.08
verigram-000	1.00	0.39	verigram-000	0.73	0.81
verigram-001	0.69	0.32	verigram-001	0.92	0.67
verihubs-inteligensia-000	0.28	0.33	verihubs-inteligensia-000	0.50	0.60
verihubs-inteligensia-001	0.13	0.29	verihubs-inteligensia-001	0.48	0.26
vida-001	0.73	0.72	vida-001	0.64	0.84

vida-002	0.23	0.18	vida-002	0.16	0.23
visteam-001	1.00	0.68	visteam-001	0.77	0.92
visteam-002	0.85	0.84	visteam-002	0.18	0.26
yoonik-001	0.51	0.52	yoonik-001	0.72	0.76
yoonik-002	0.95	1.00	yoonik-002	0.53	0.74
yoti-001	1.00	1.00	yoti-001	1.00	0.22
yoti-002	1.00	1.00	yoti-002	1.00	0.24

Fig. 46. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

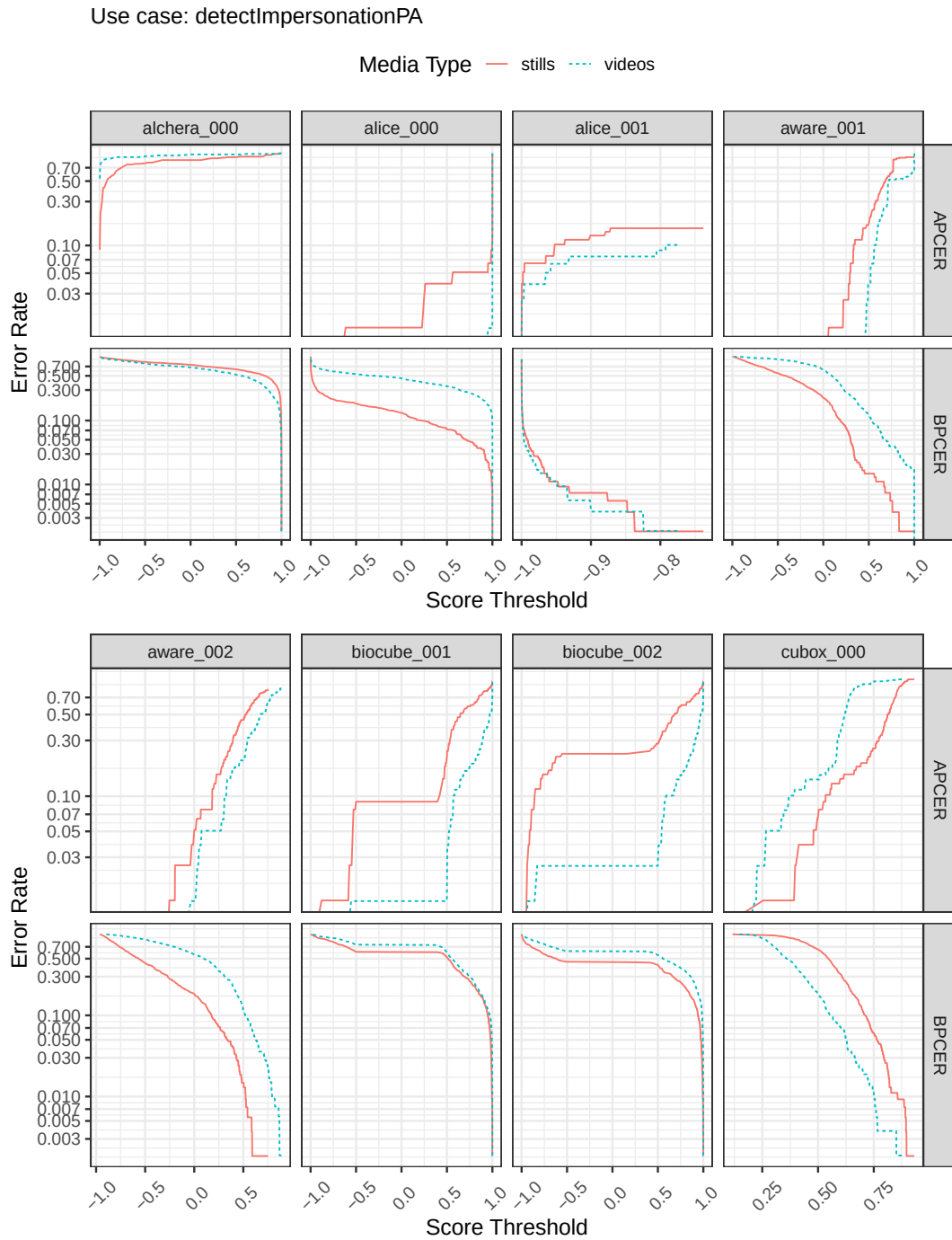


Fig. 47. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

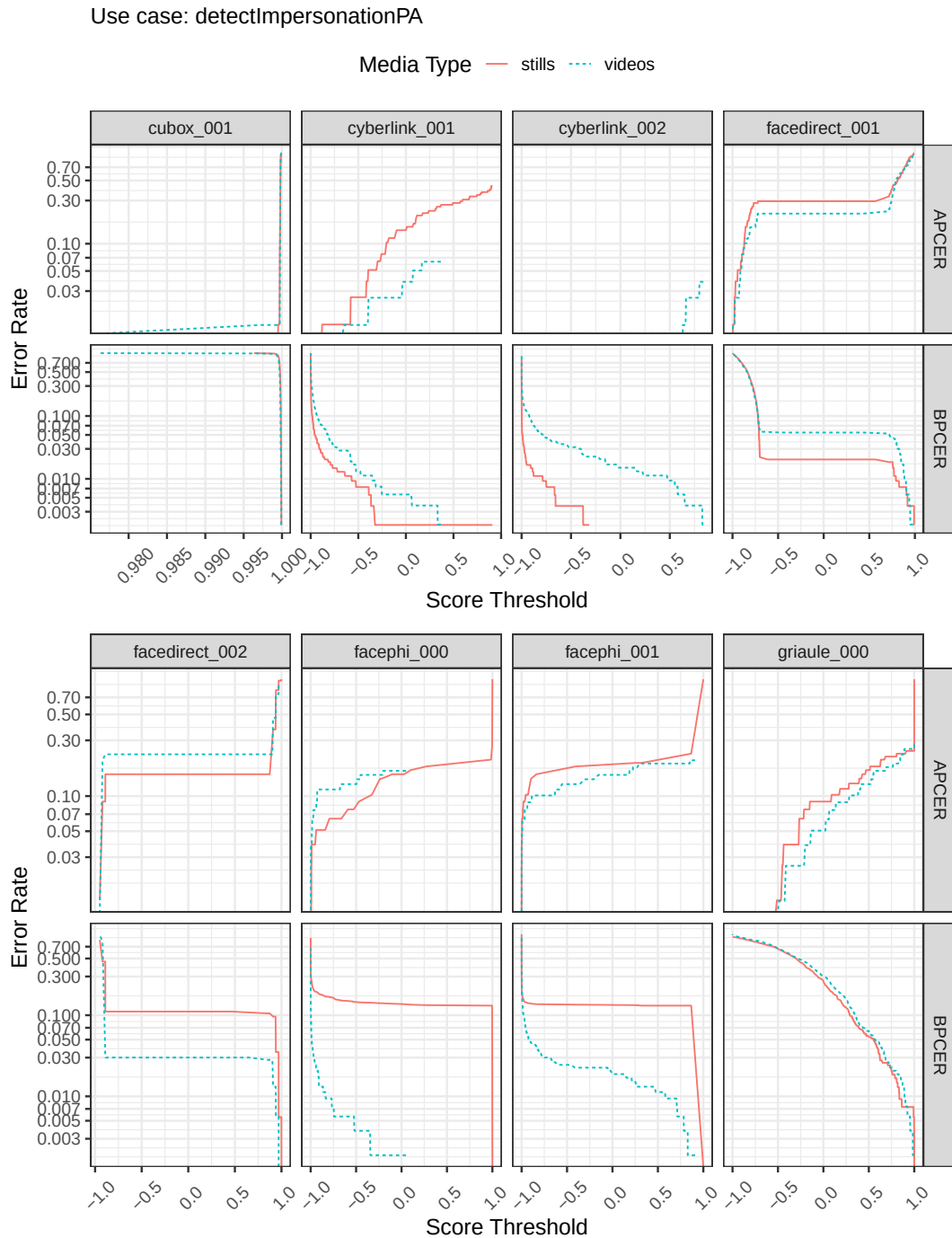


Fig. 48. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

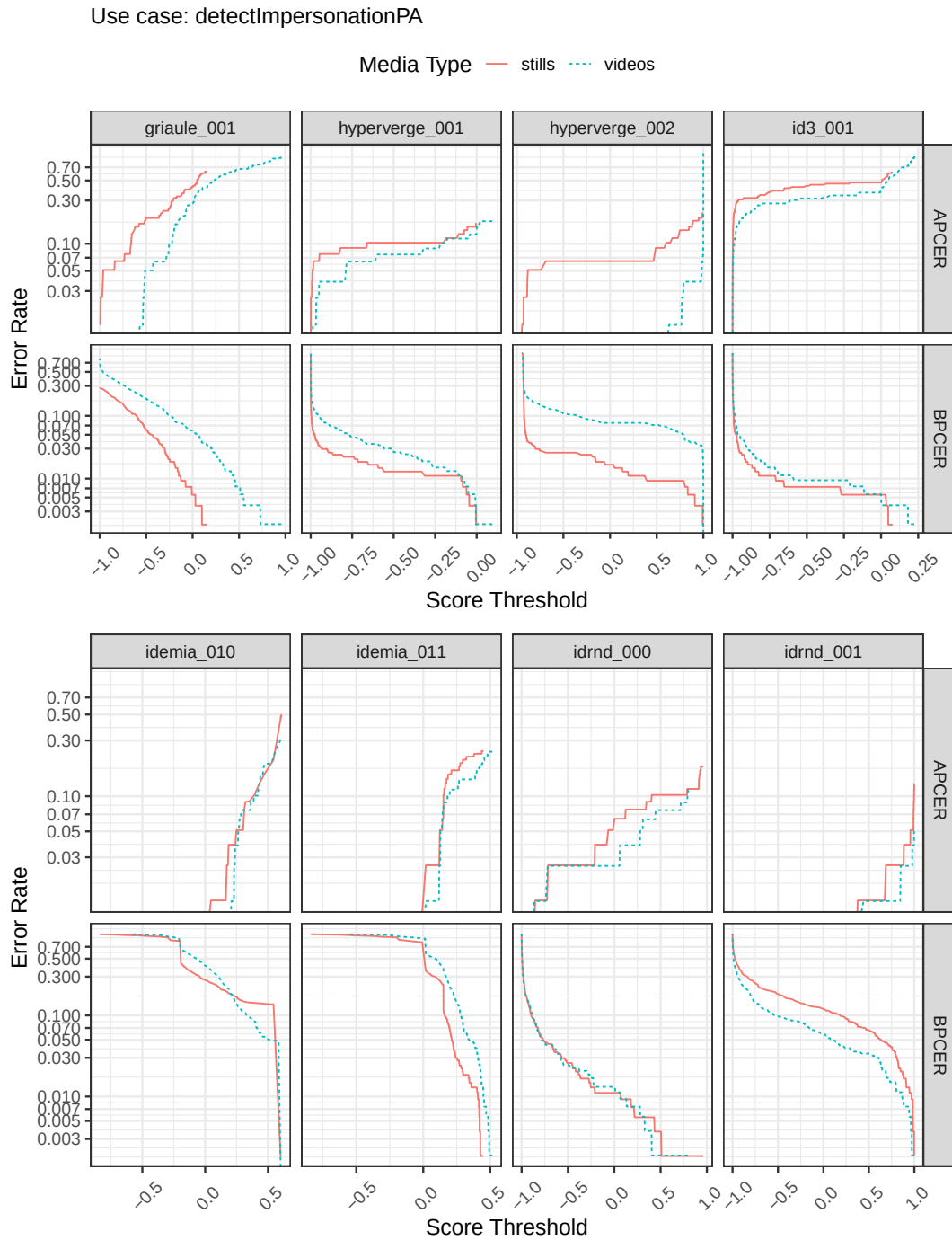


Fig. 49. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

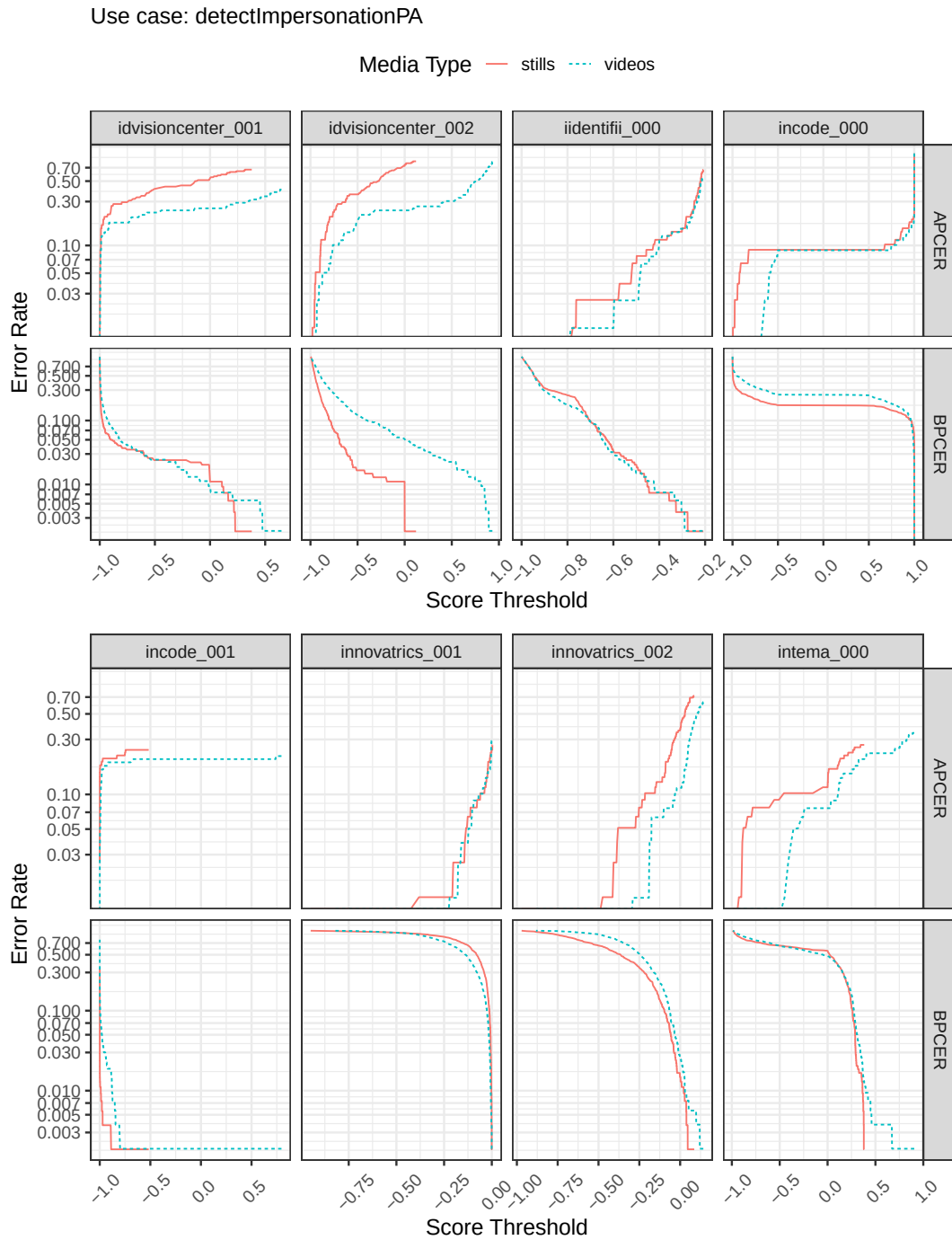


Fig. 50. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

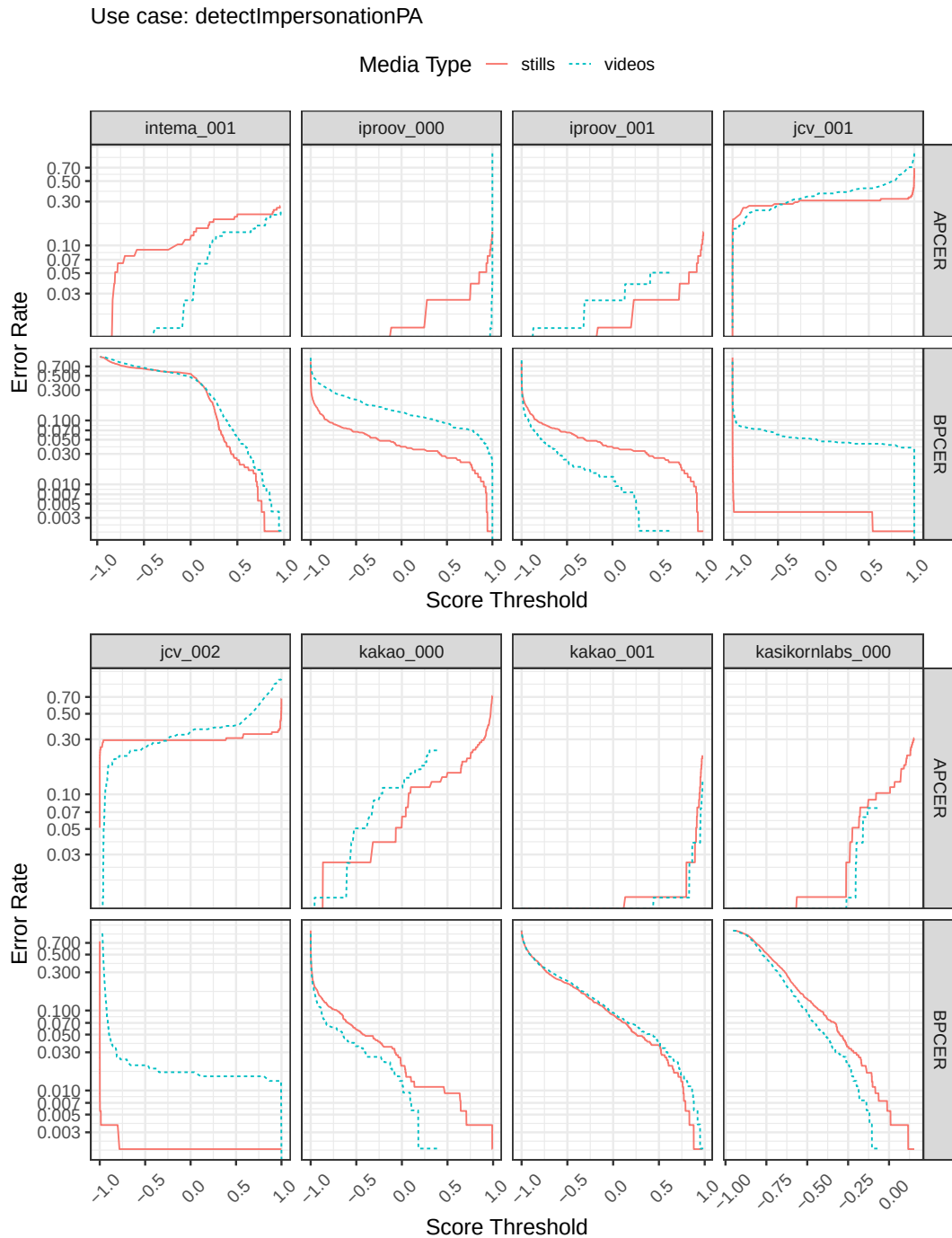


Fig. 51. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

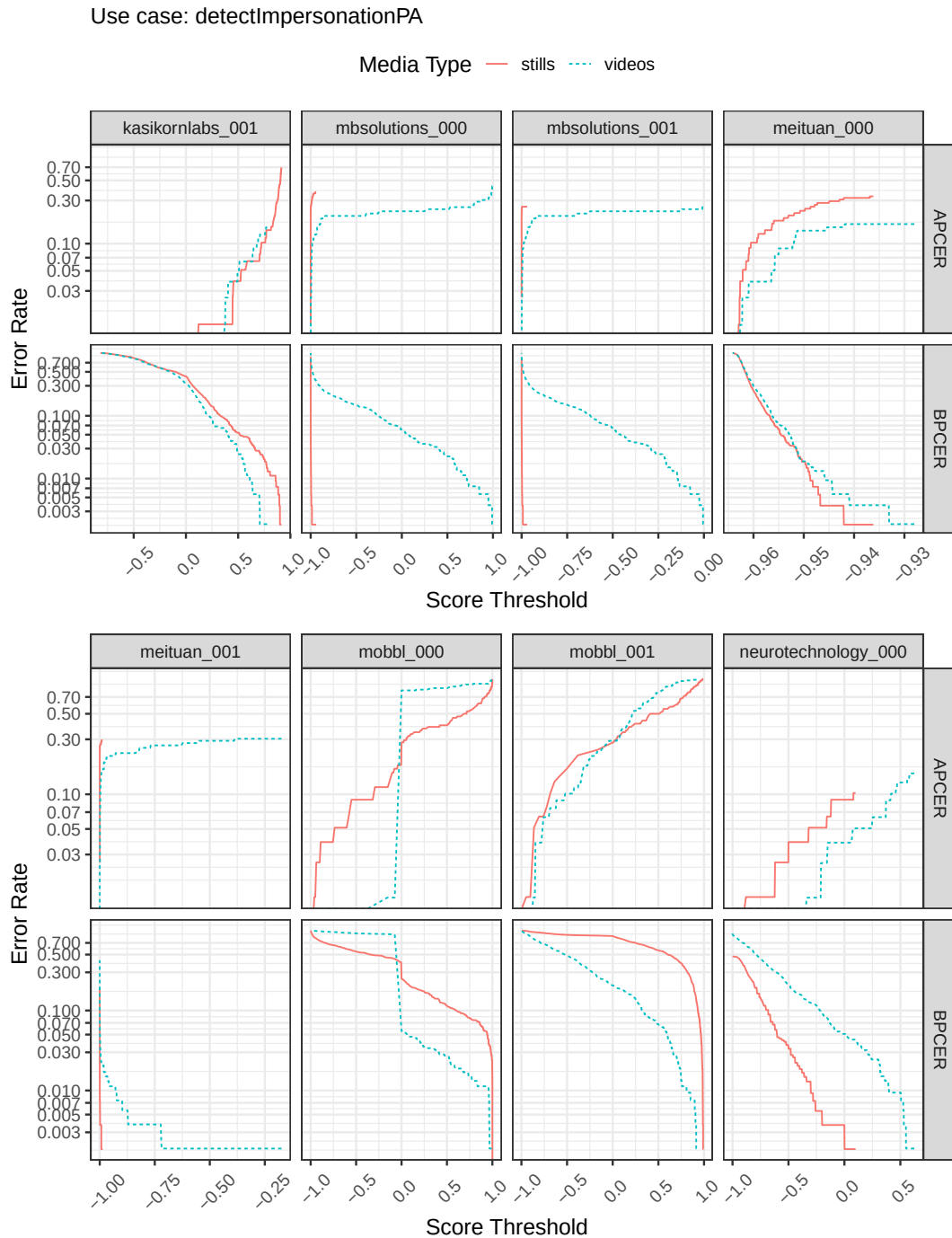


Fig. 52. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

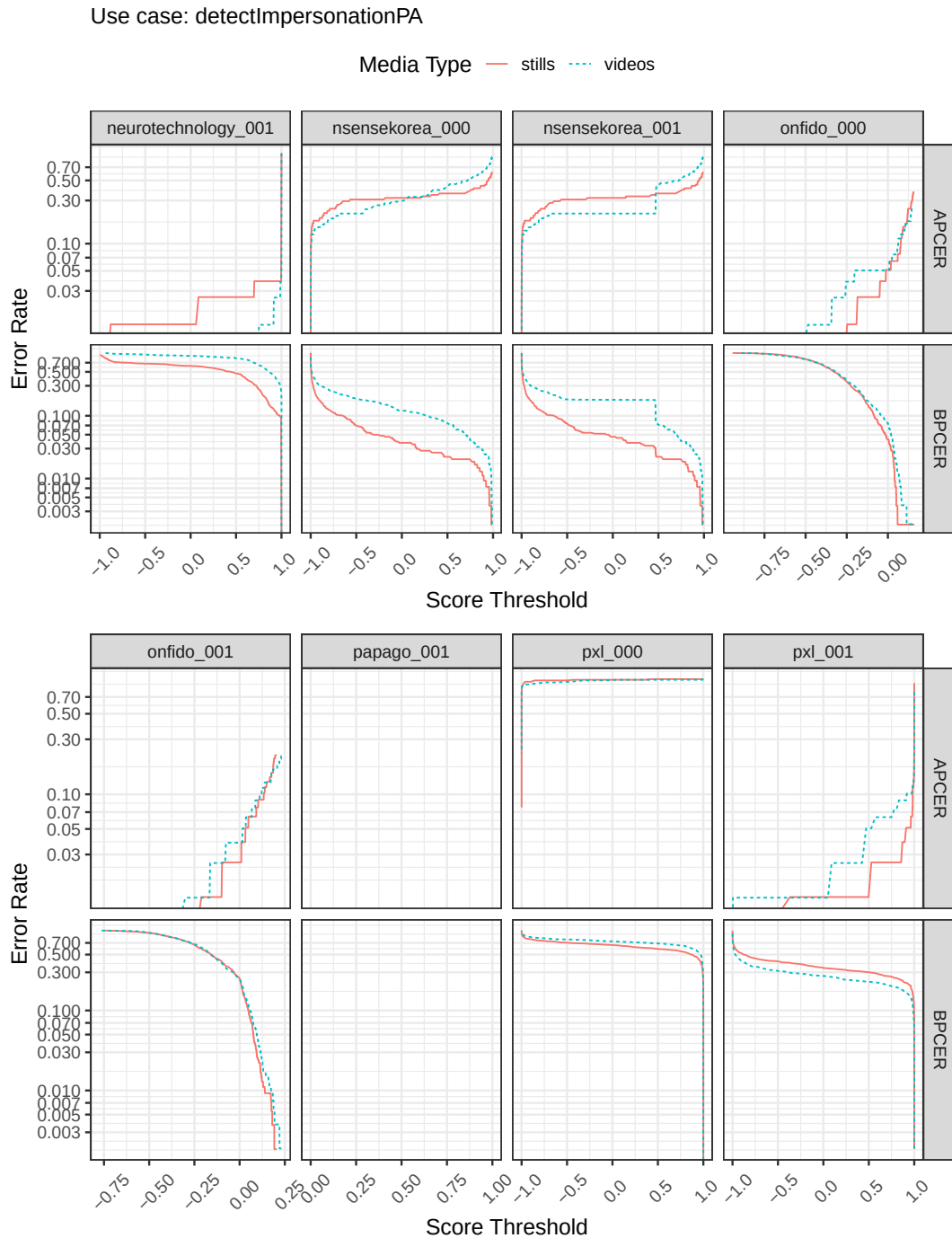


Fig. 53. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

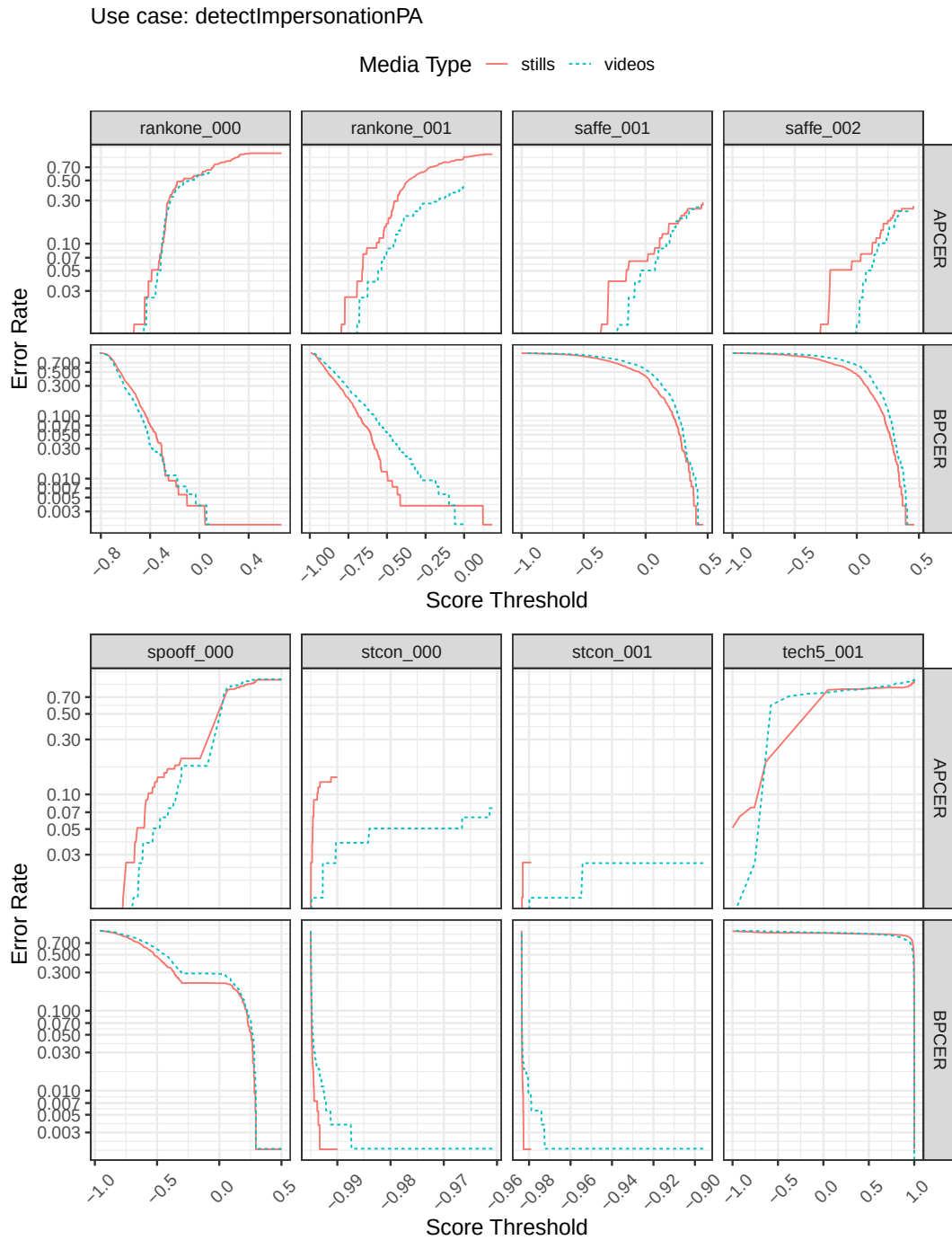


Fig. 54. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

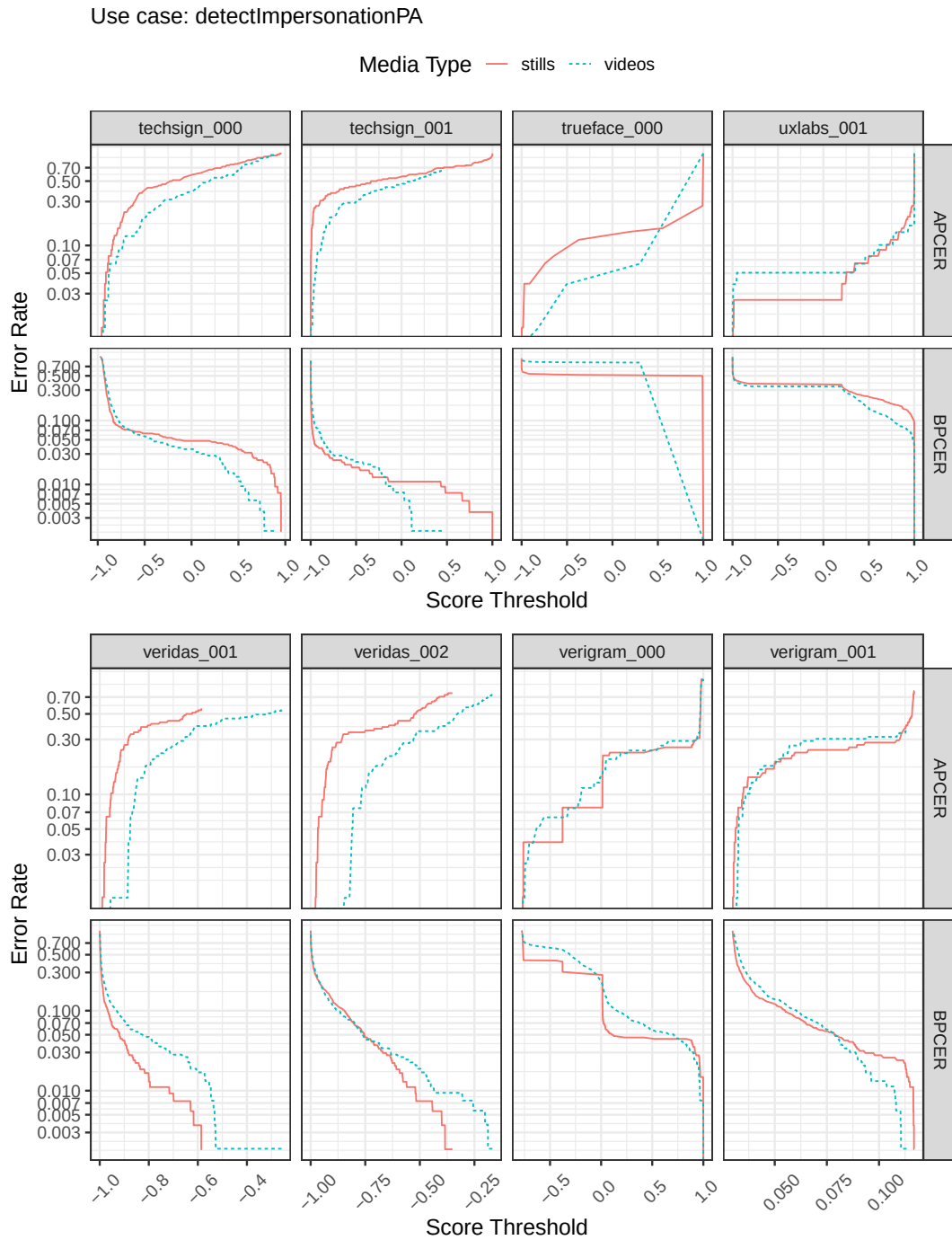


Fig. 55. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

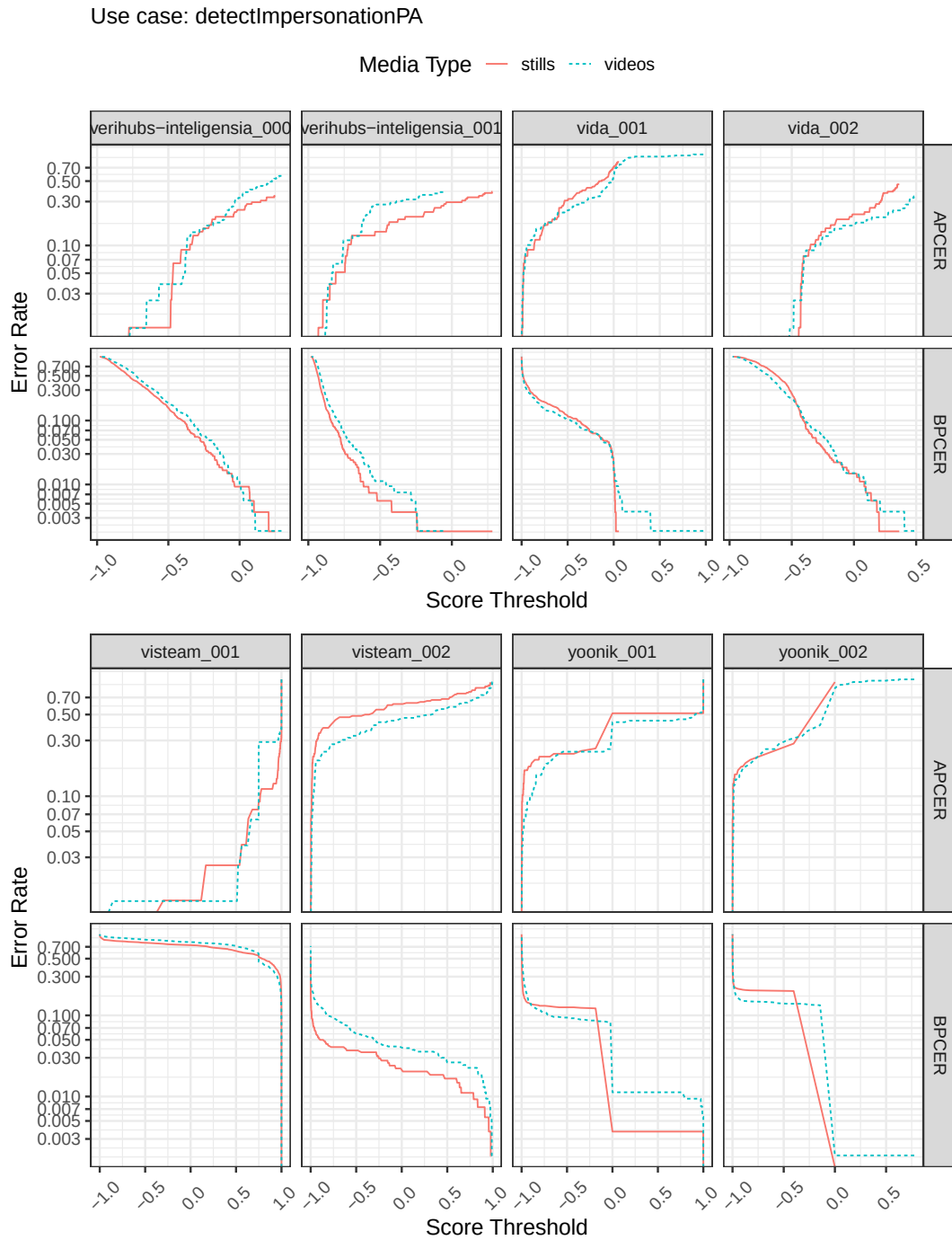
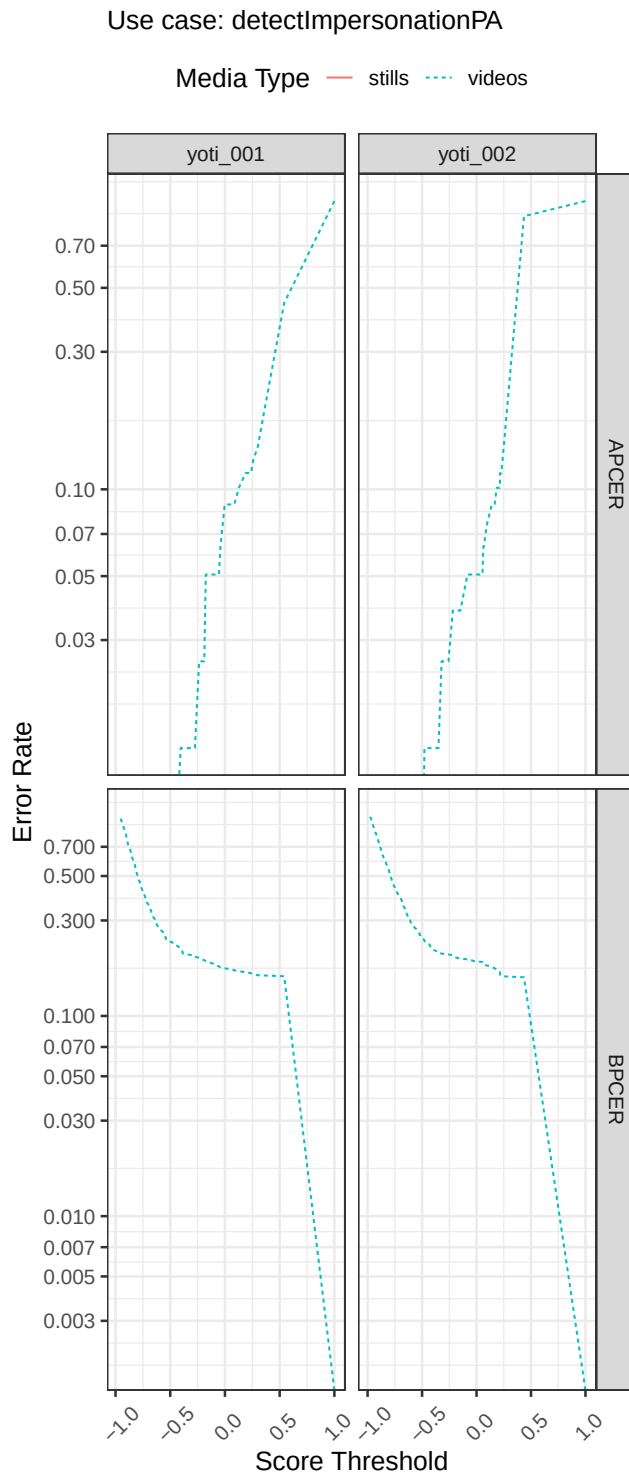


Fig. 56. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.



Appendix B.2. Evasion

Table 55. Use Case: detectEvasionPA - Stills vs. Videos

Algorithm	(Convenience) APCER @ BPCER=0.01		Algorithm	(Security) BPCER @ APCER=0.01	
	Stills	Videos		Stills	Videos
alchera-000	1.00	1.00	alchera-000	1.00	1.00
alice-000	0.49	1.00	alice-000	0.49	0.62
aware-001	0.52	0.82	aware-001	0.49	0.57
aware-002	0.68	0.81	aware-002	0.51	0.72
cubox-000	0.96	0.95	cubox-000	0.98	0.95
cubox-001	0.95	0.93	cubox-001	0.99	0.97
cyberlink-001	0.92	0.86	cyberlink-001	0.85	0.84
cyberlink-002	0.75	0.52	cyberlink-002	0.24	0.28
facedirect-001	0.80	0.88	facedirect-001	0.98	0.92
facedirect-002	0.83	0.72	facedirect-002	1.00	1.00
griaule-000	0.90	0.89	griaule-000	0.99	1.00
griaule-001	0.91	0.90	griaule-001	0.95	0.98
jcv-001	1.00	1.00	jcv-001	0.99	1.00
kakao-000	0.25	0.19	kakao-000	0.16	0.17
kakao-001	0.11	0.04	kakao-001	0.11	0.03
kasikornlabs-000	0.38	0.32	kasikornlabs-000	0.84	0.90
kasikornlabs-001	0.47	0.36	kasikornlabs-001	0.84	0.88
neurotechnology-000	0.37	0.44	neurotechnology-000	1.00	0.57
neurotechnology-001	1.00	1.00	neurotechnology-001	0.82	0.89
onfido-000	0.36	0.38	onfido-000	0.74	0.81
onfido-001	0.53	0.49	onfido-001	0.77	0.71
papago-001	1.00	1.00	papago-001	1.00	1.00
rankone-000	0.75	0.89	rankone-000	0.92	0.92
rankone-001	0.75	0.89	rankone-001	0.92	0.92
spooff-000	1.00	1.00	spooff-000	1.00	1.00
trueface-000	0.97	0.96	trueface-000	1.00	1.00
uxlabs-001	1.00	1.00	uxlabs-001	0.48	0.51

Fig. 57. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

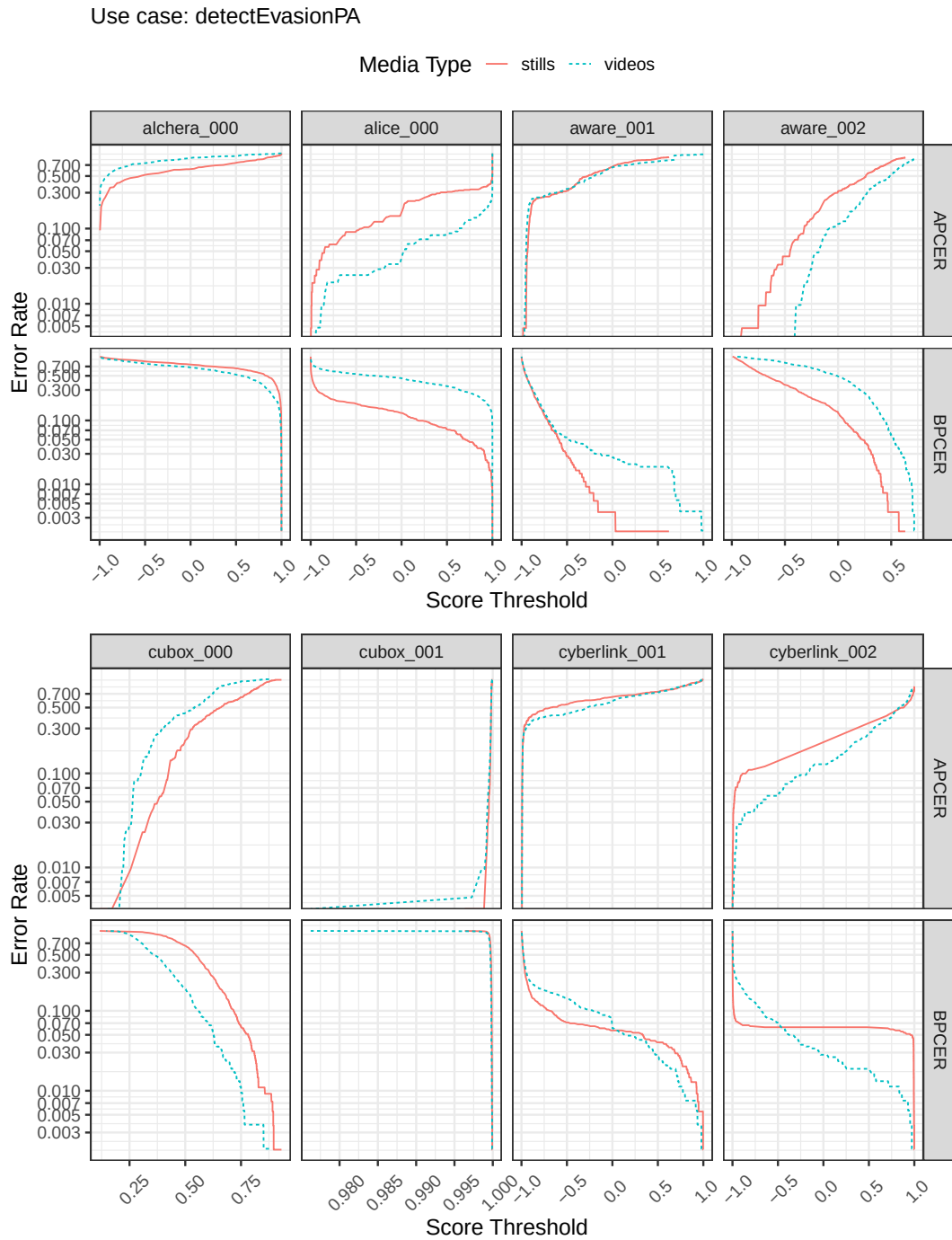


Fig. 58. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

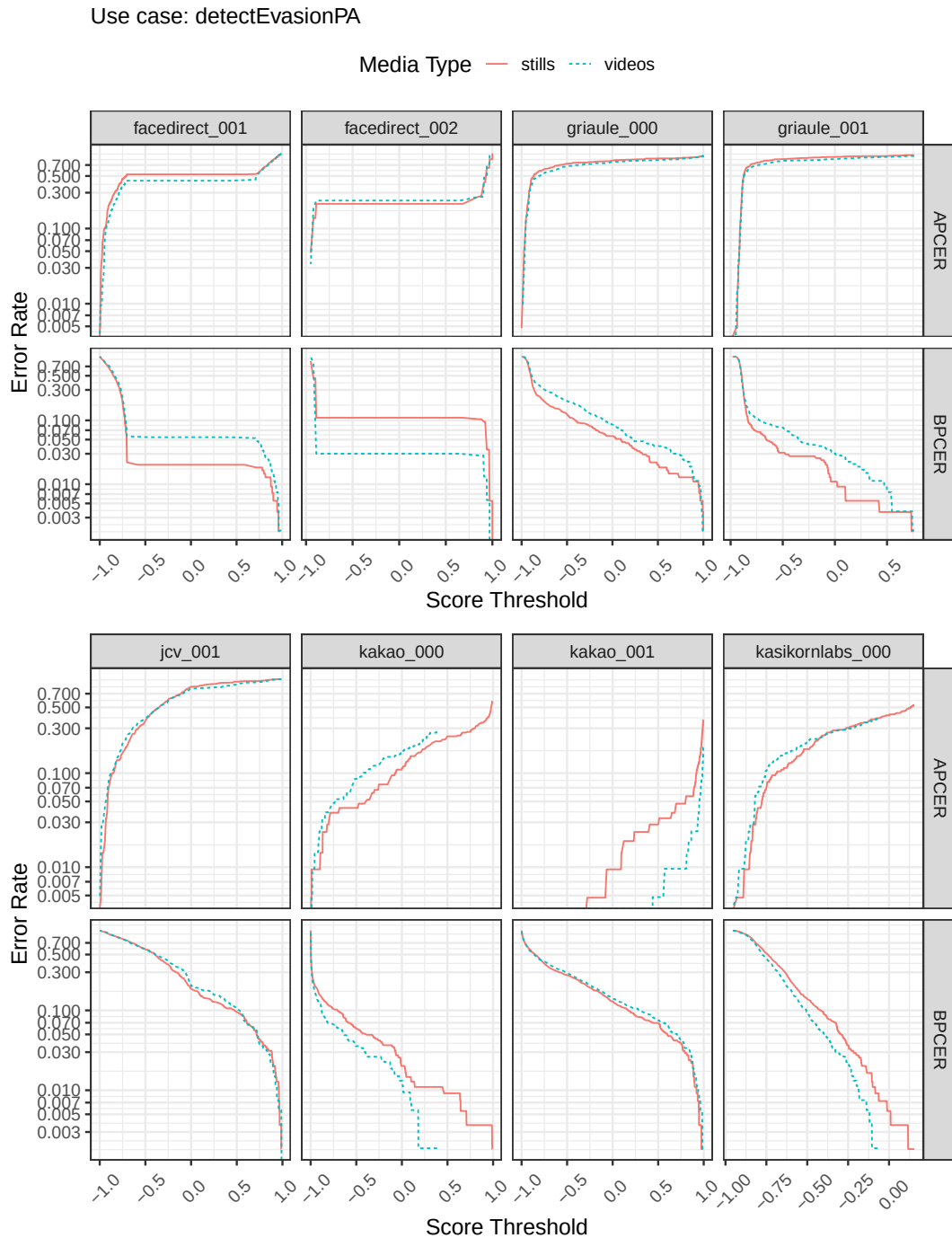


Fig. 59. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.

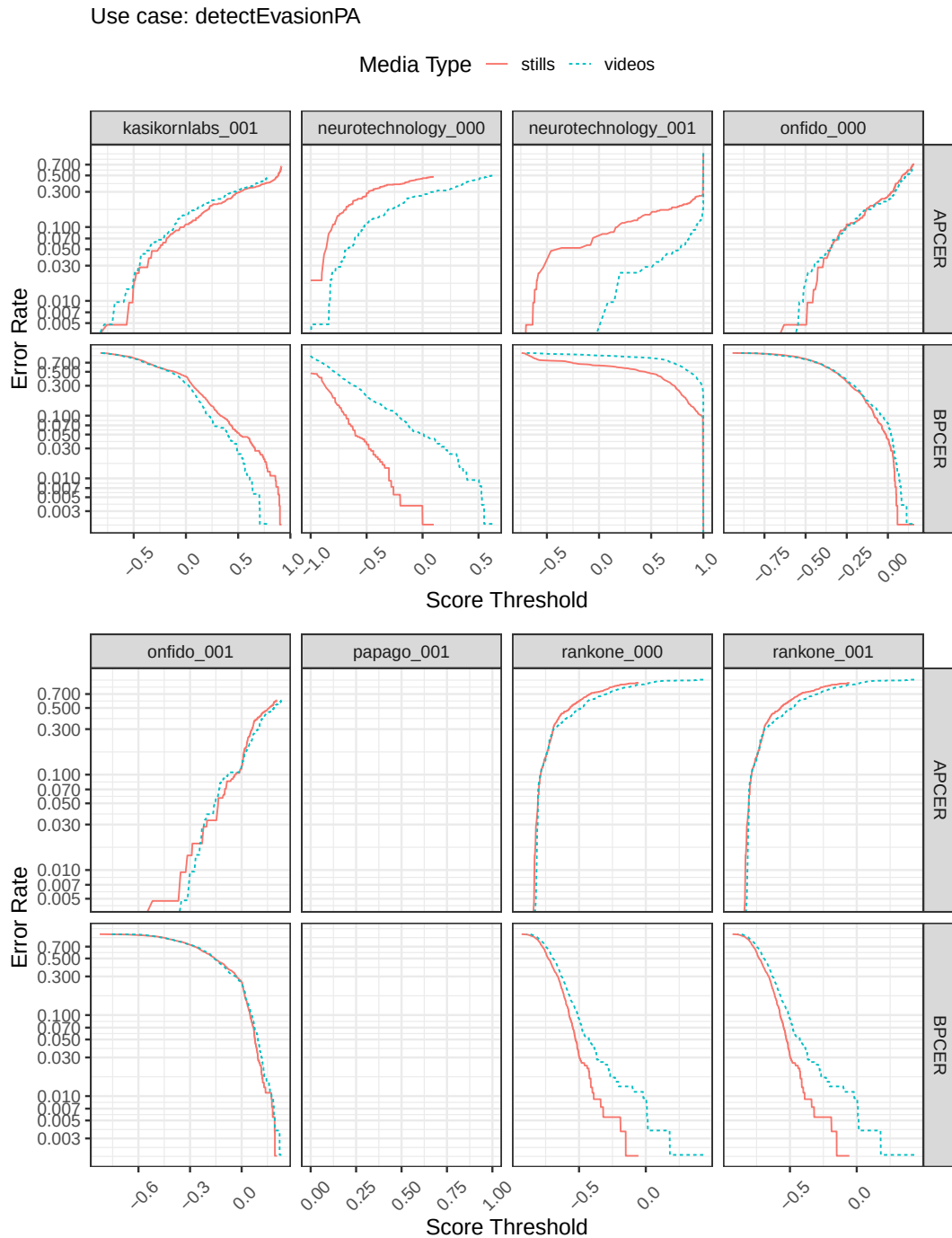
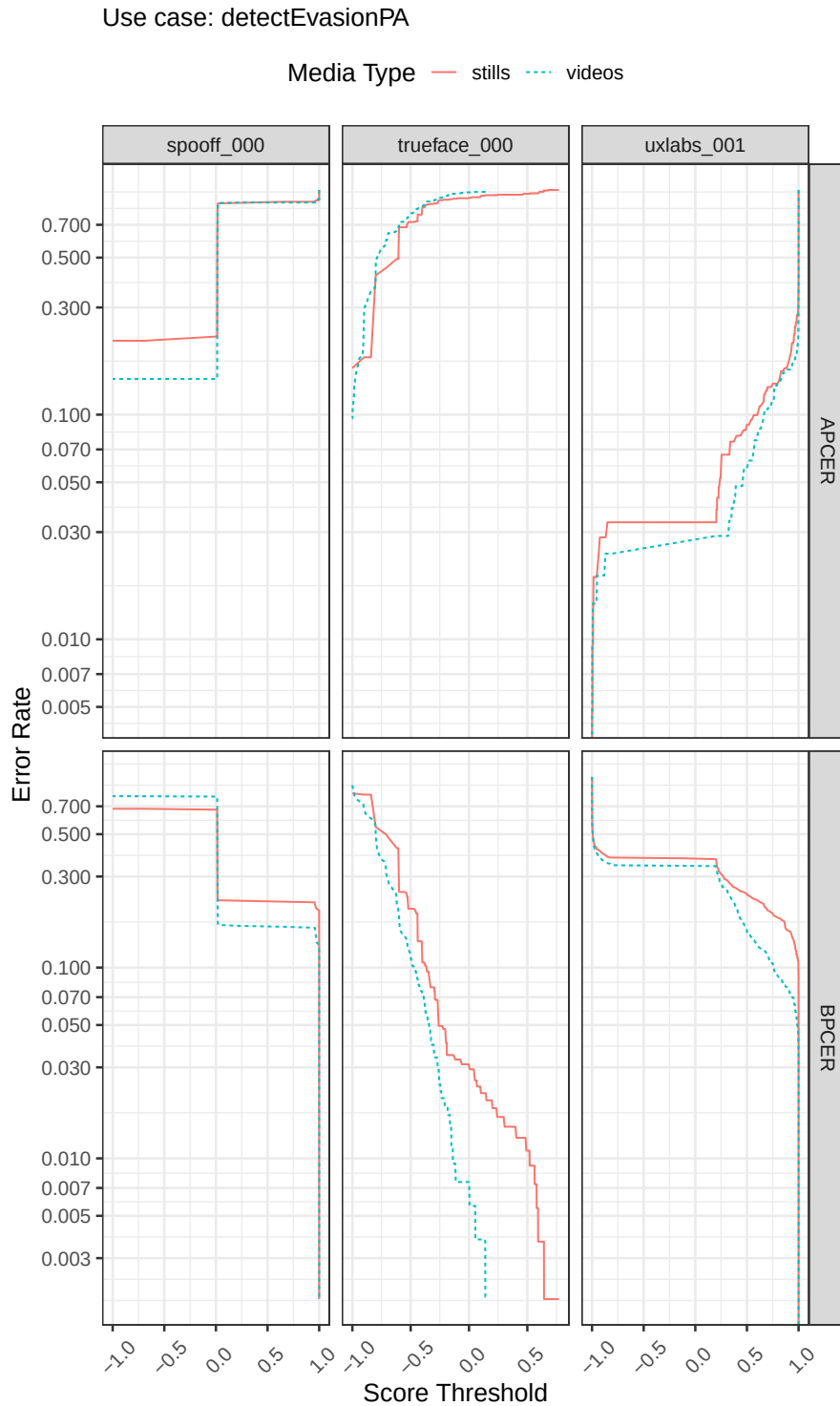


Fig. 60. This plot presents APCER and BPCER as a function of threshold on still images vs. videos.



Appendix C. Demographic Effects

Appendix C.1. Impersonation

Fig. 61. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

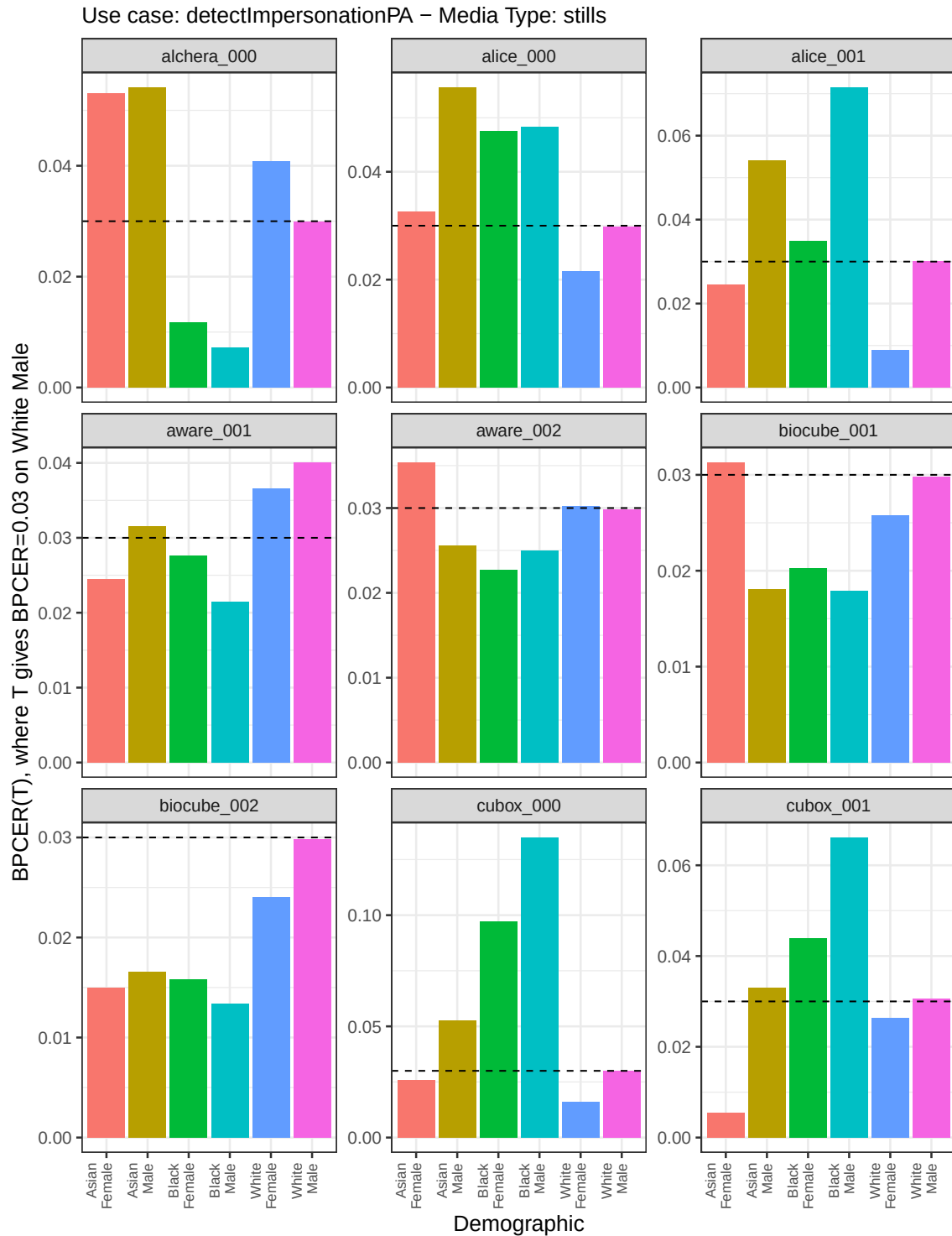


Fig. 62. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

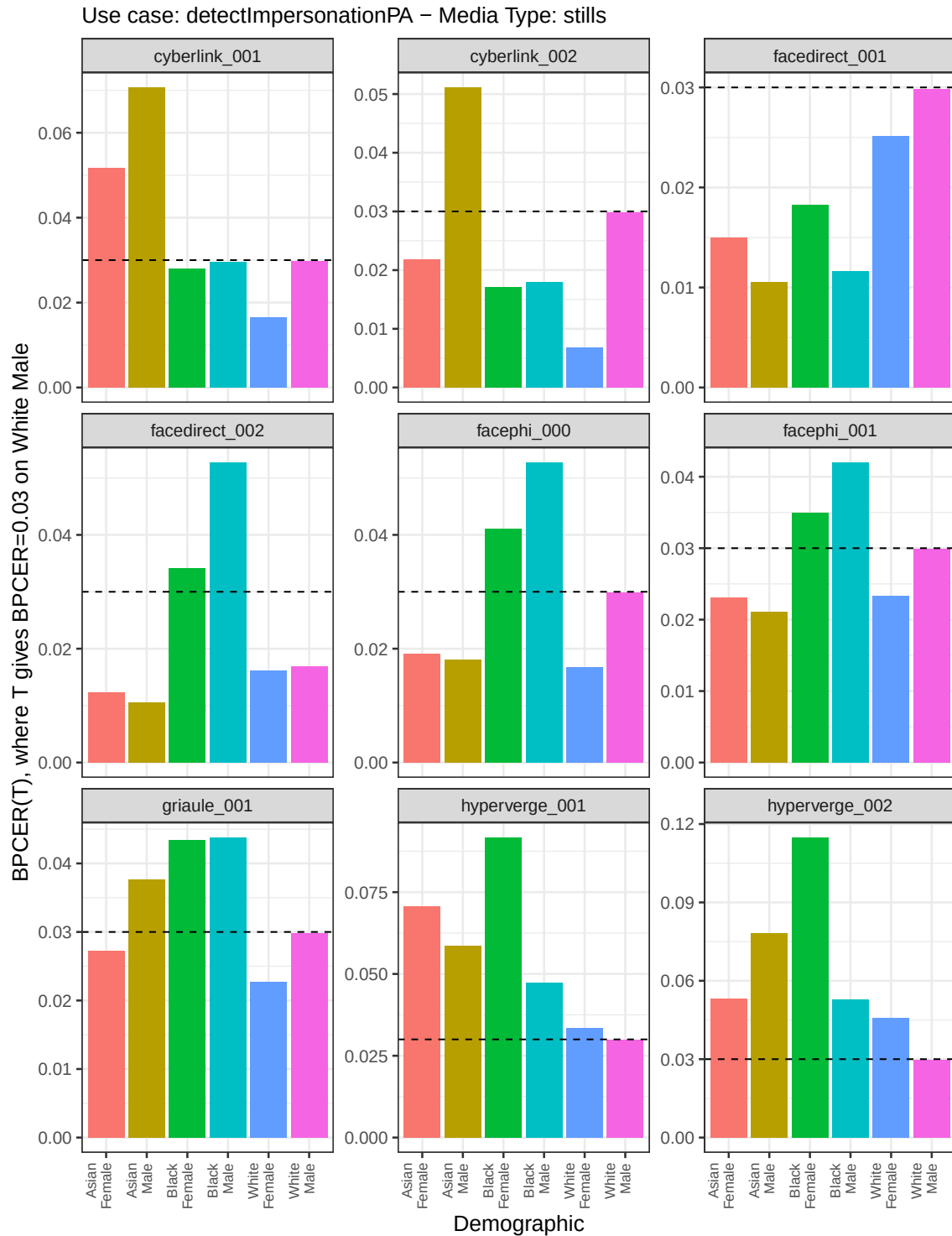


Fig. 63. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

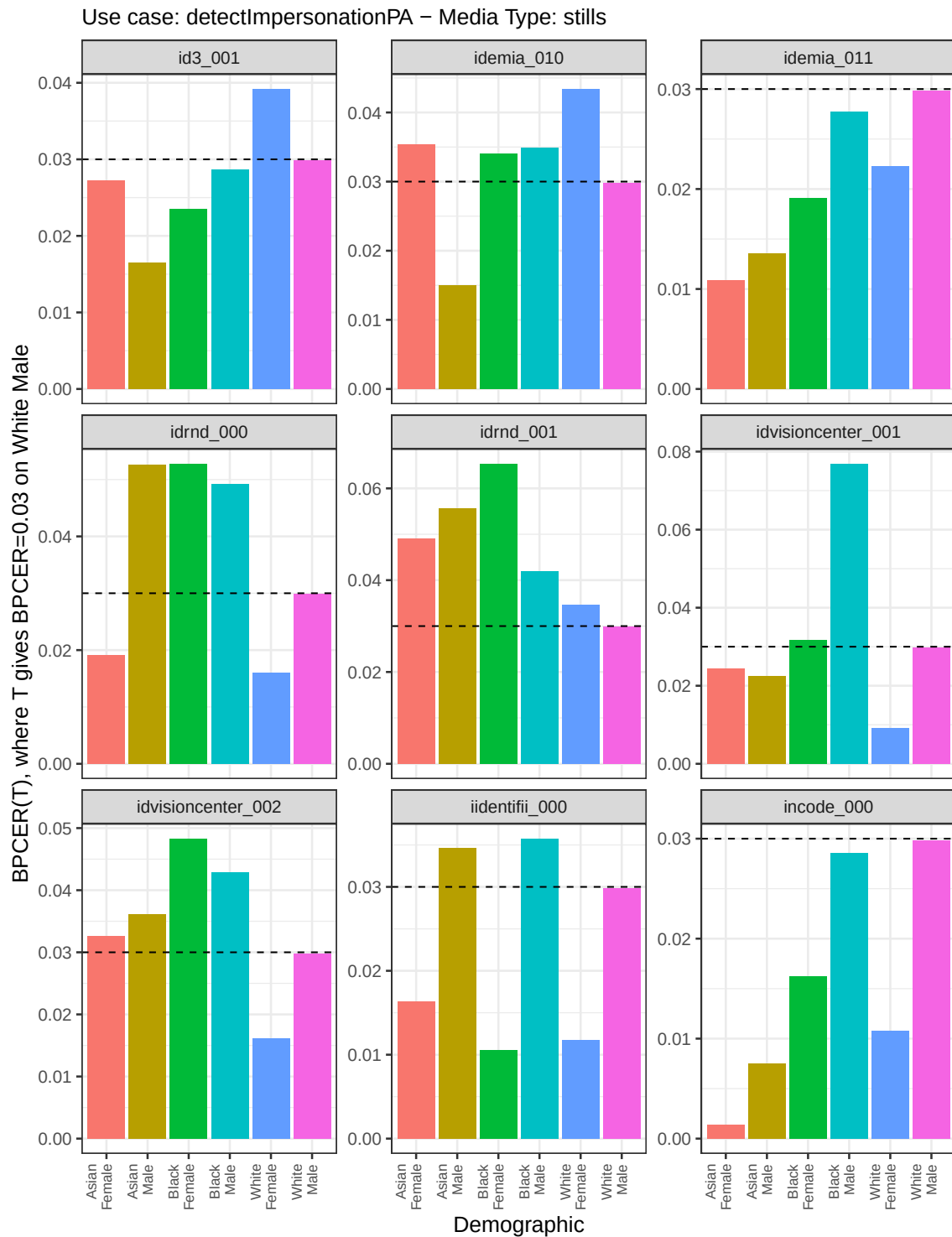


Fig. 64. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

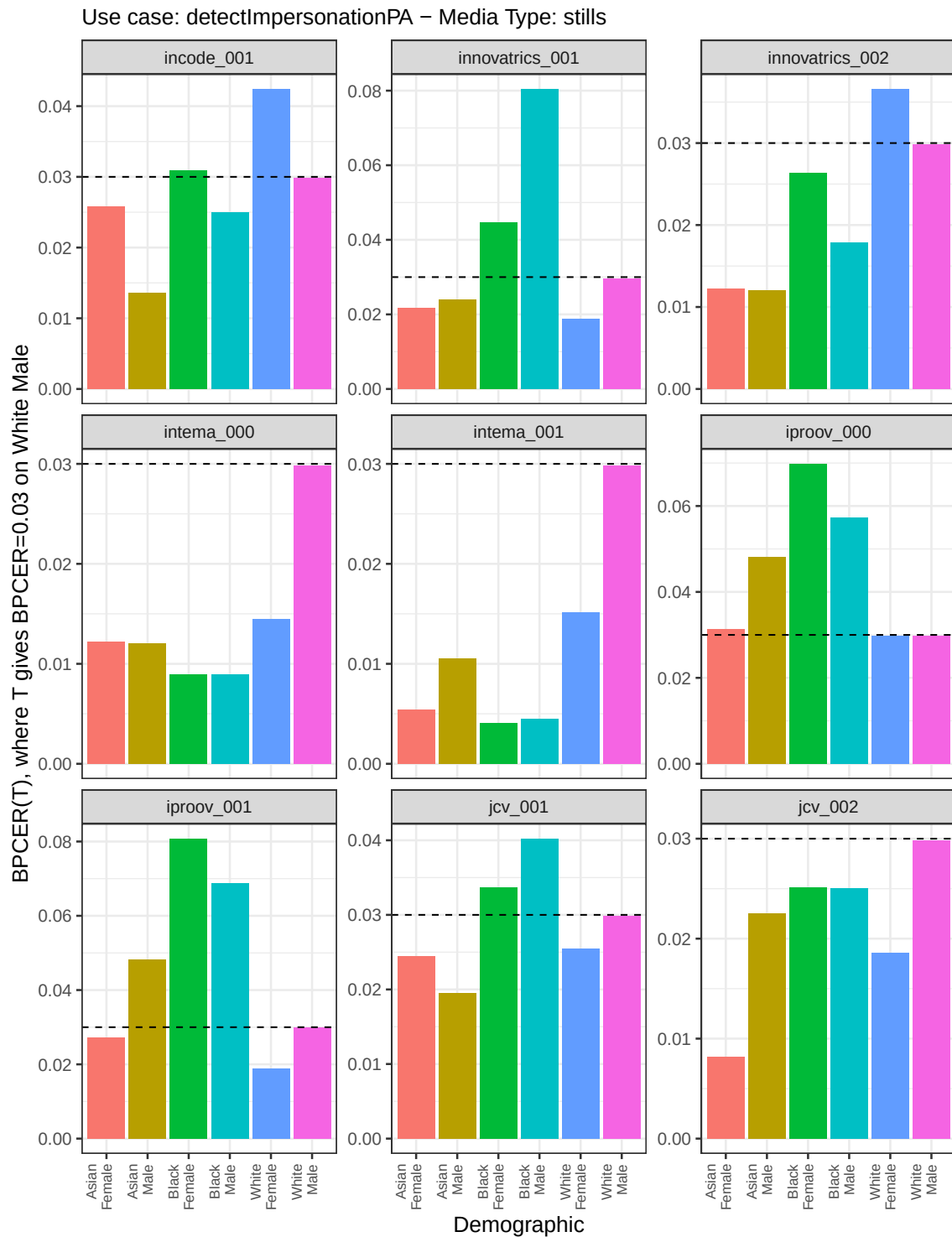


Fig. 65. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

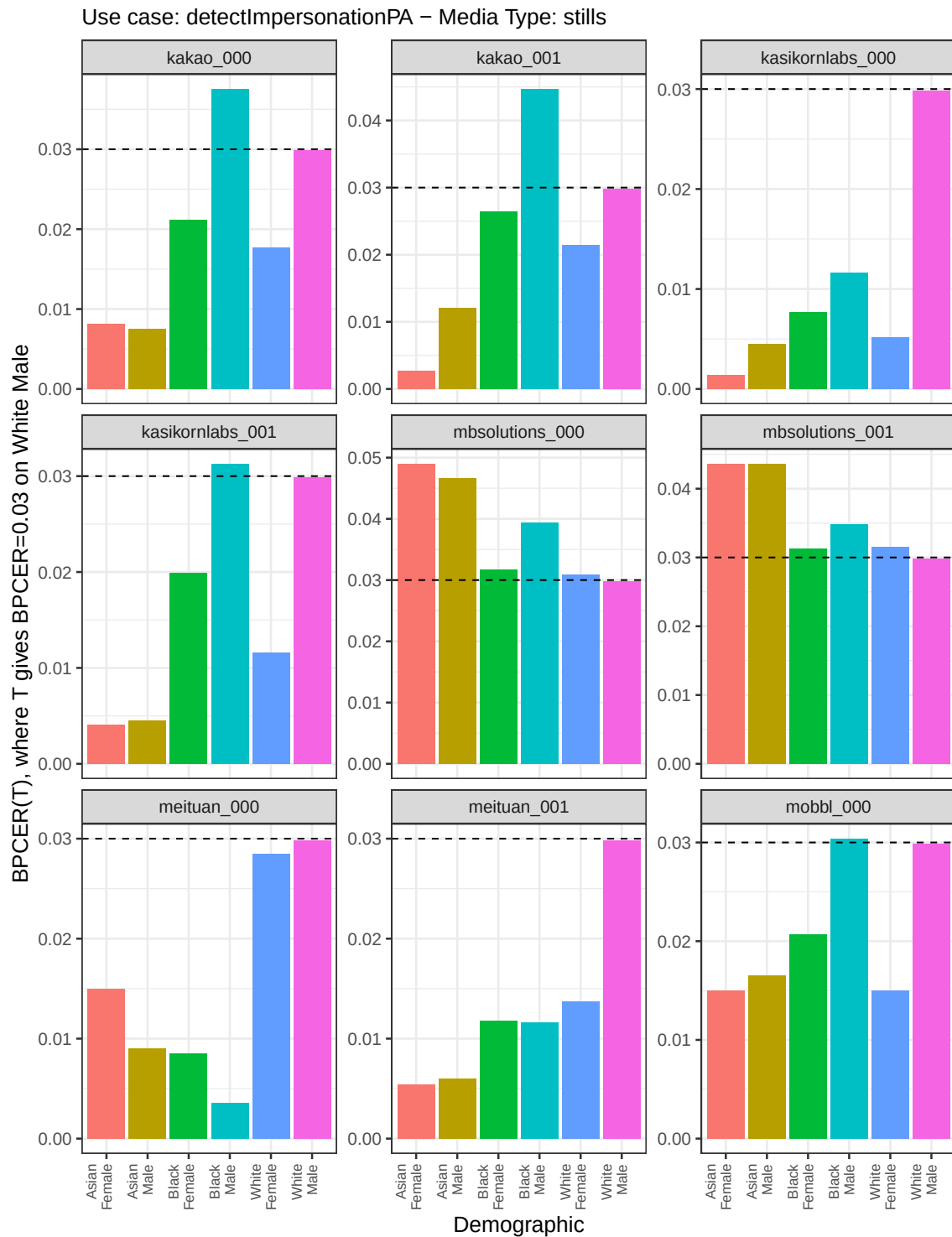


Fig. 66. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

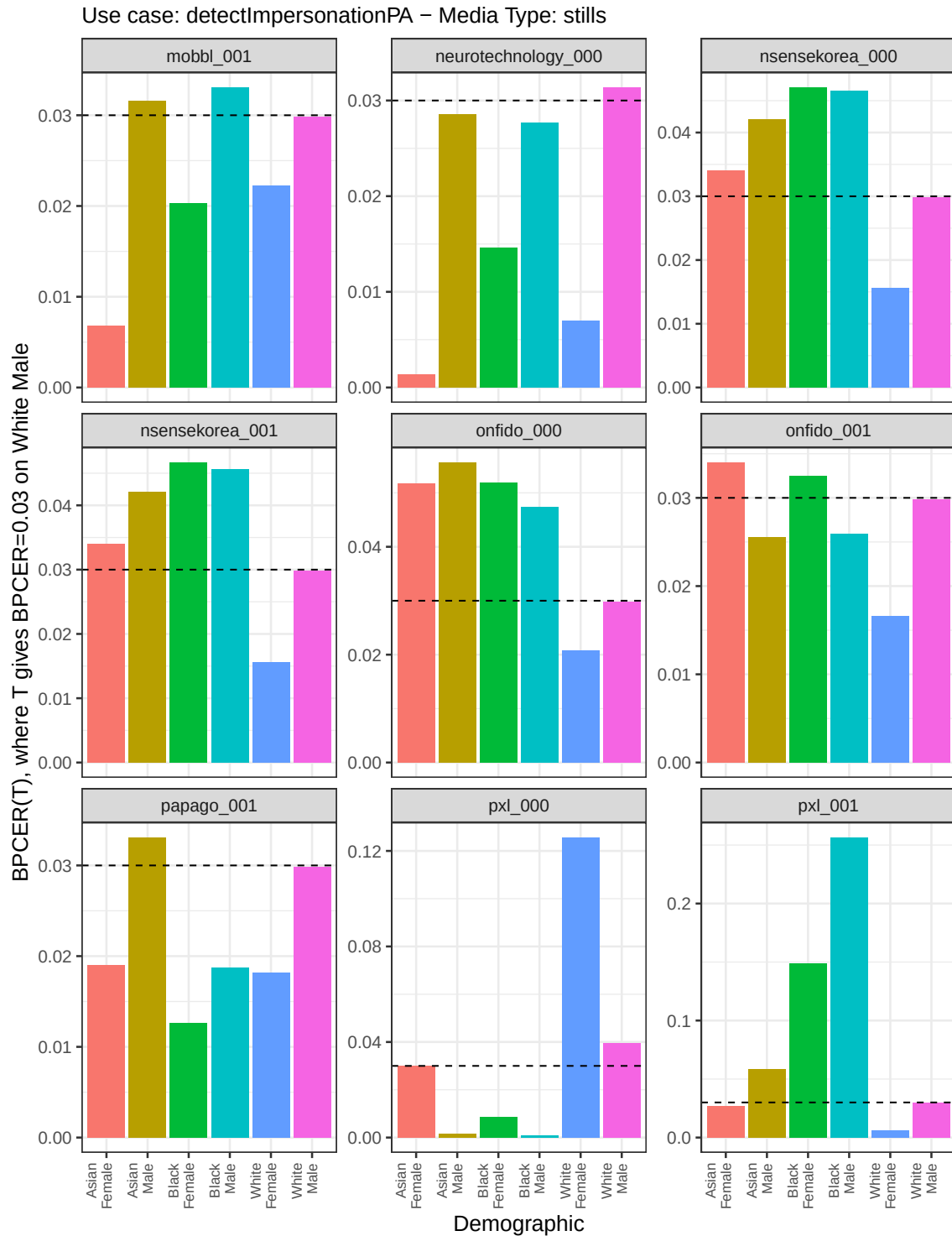


Fig. 67. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

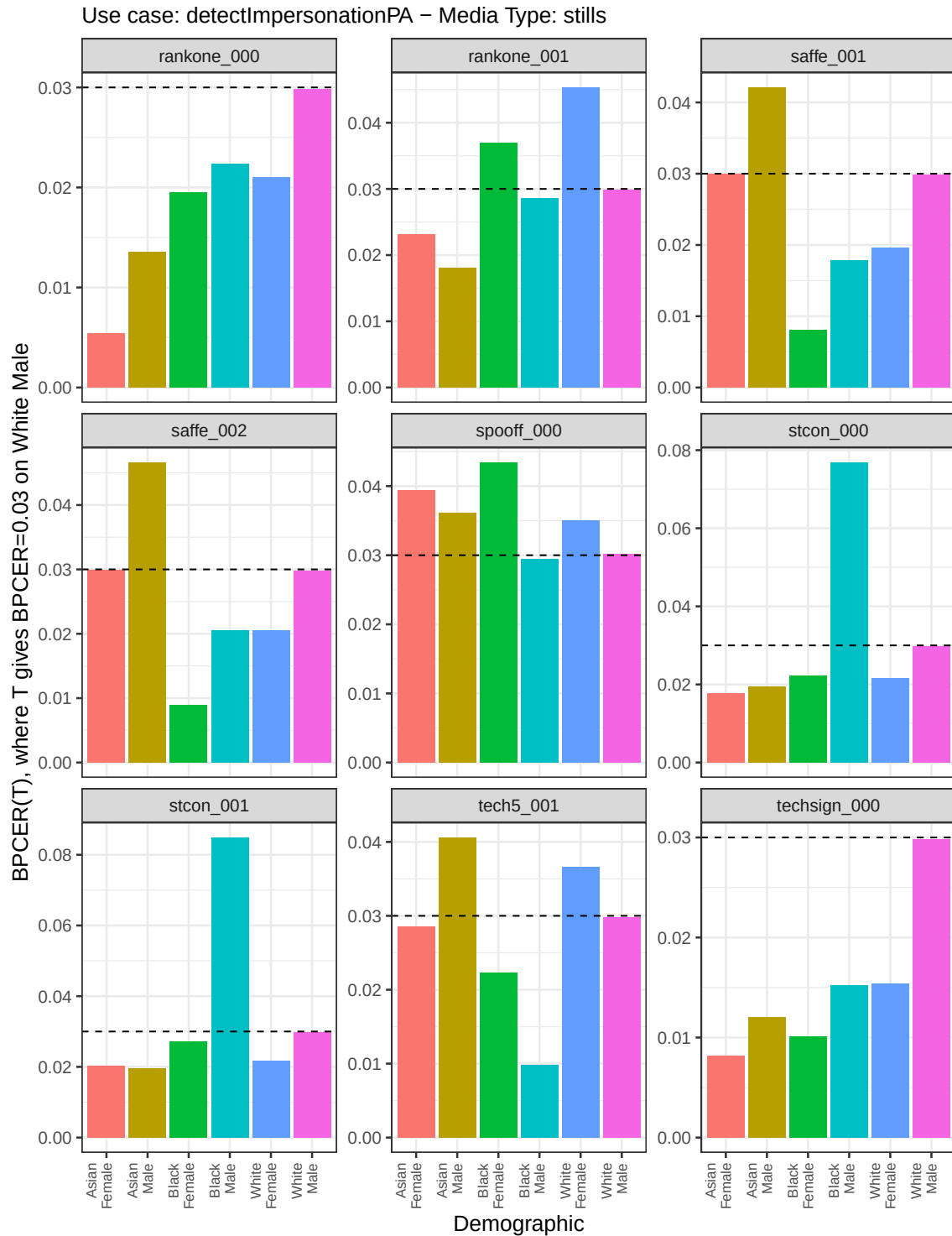


Fig. 68. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

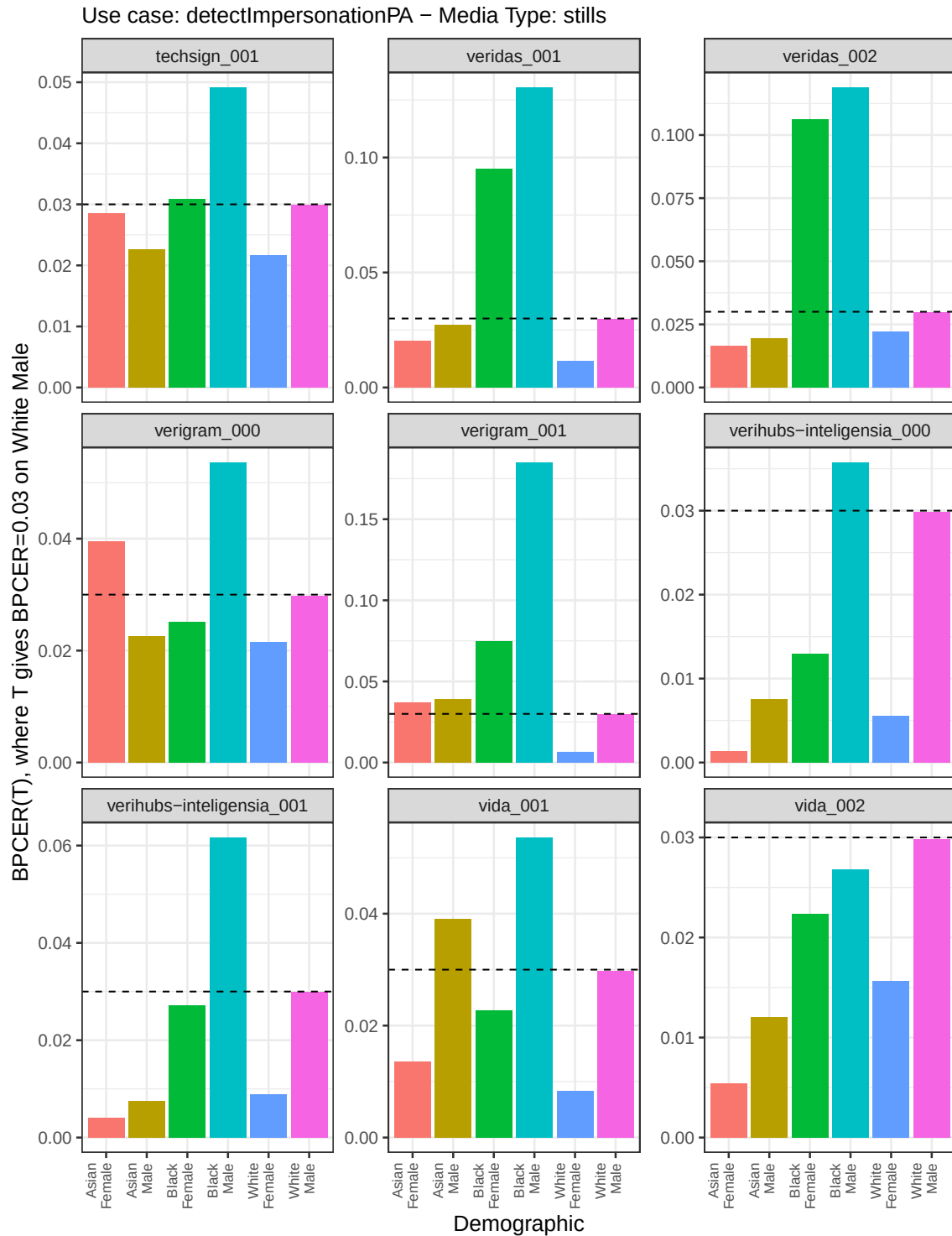
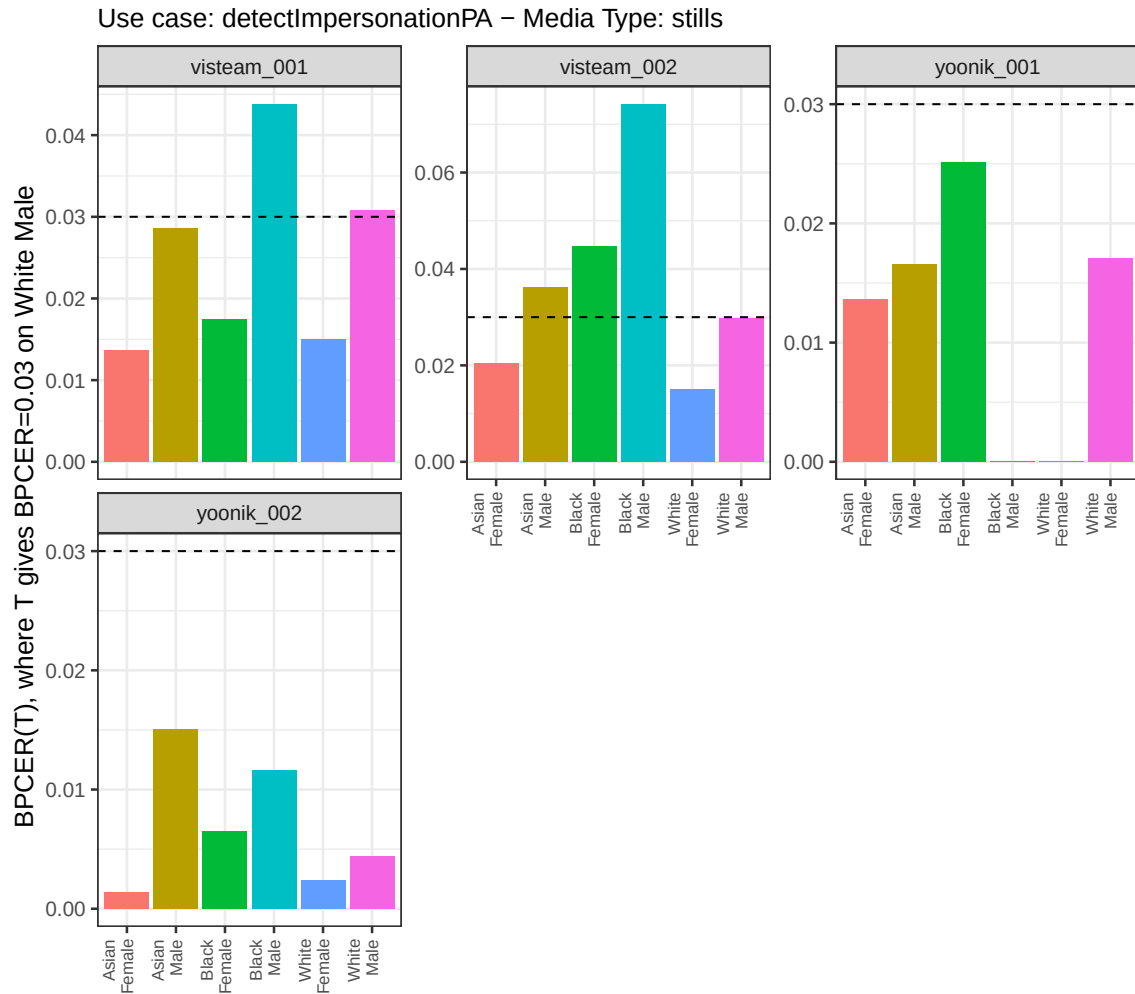


Fig. 69. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.



Demographic

Appendix C.2. Evasion

Fig. 70. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

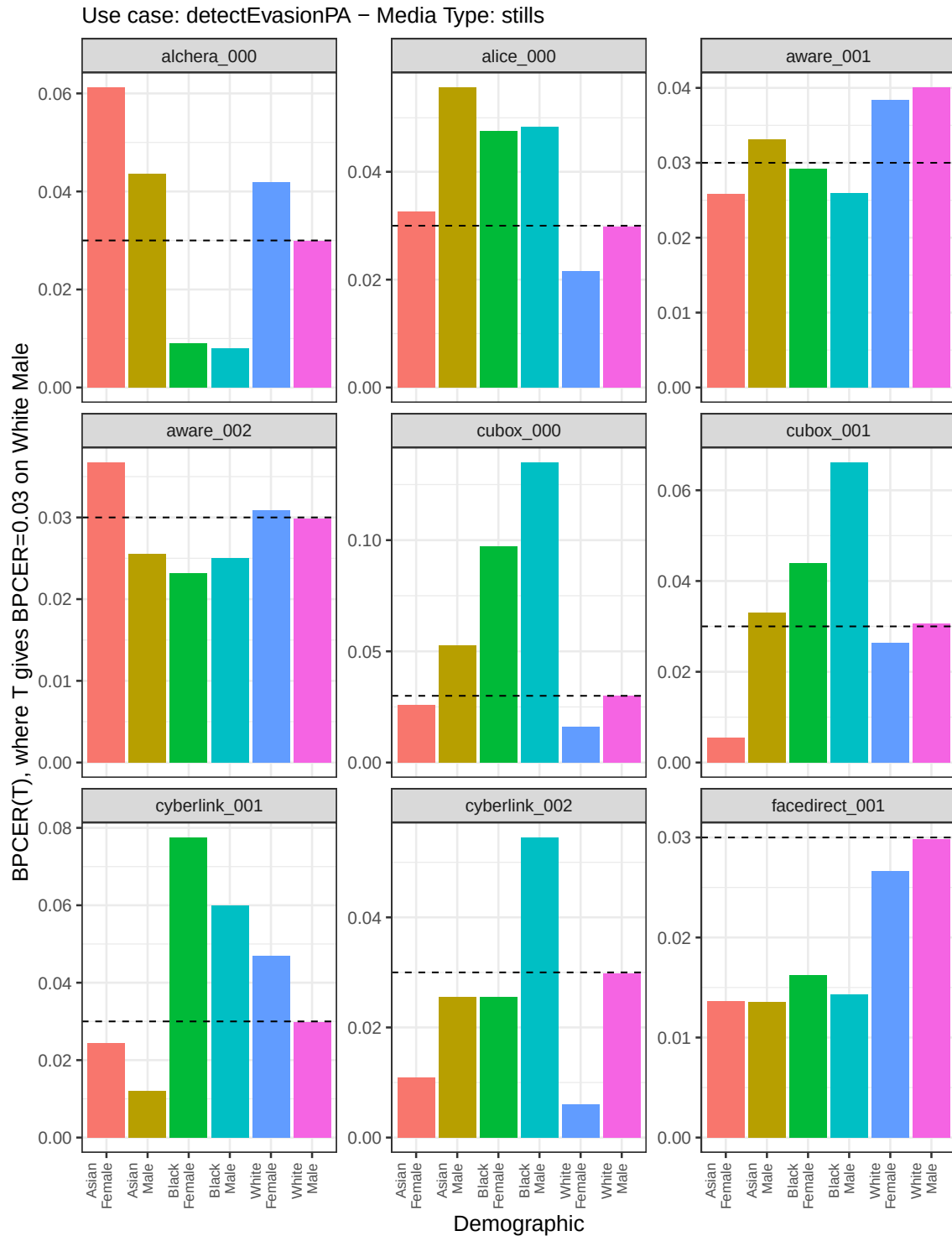


Fig. 71. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.

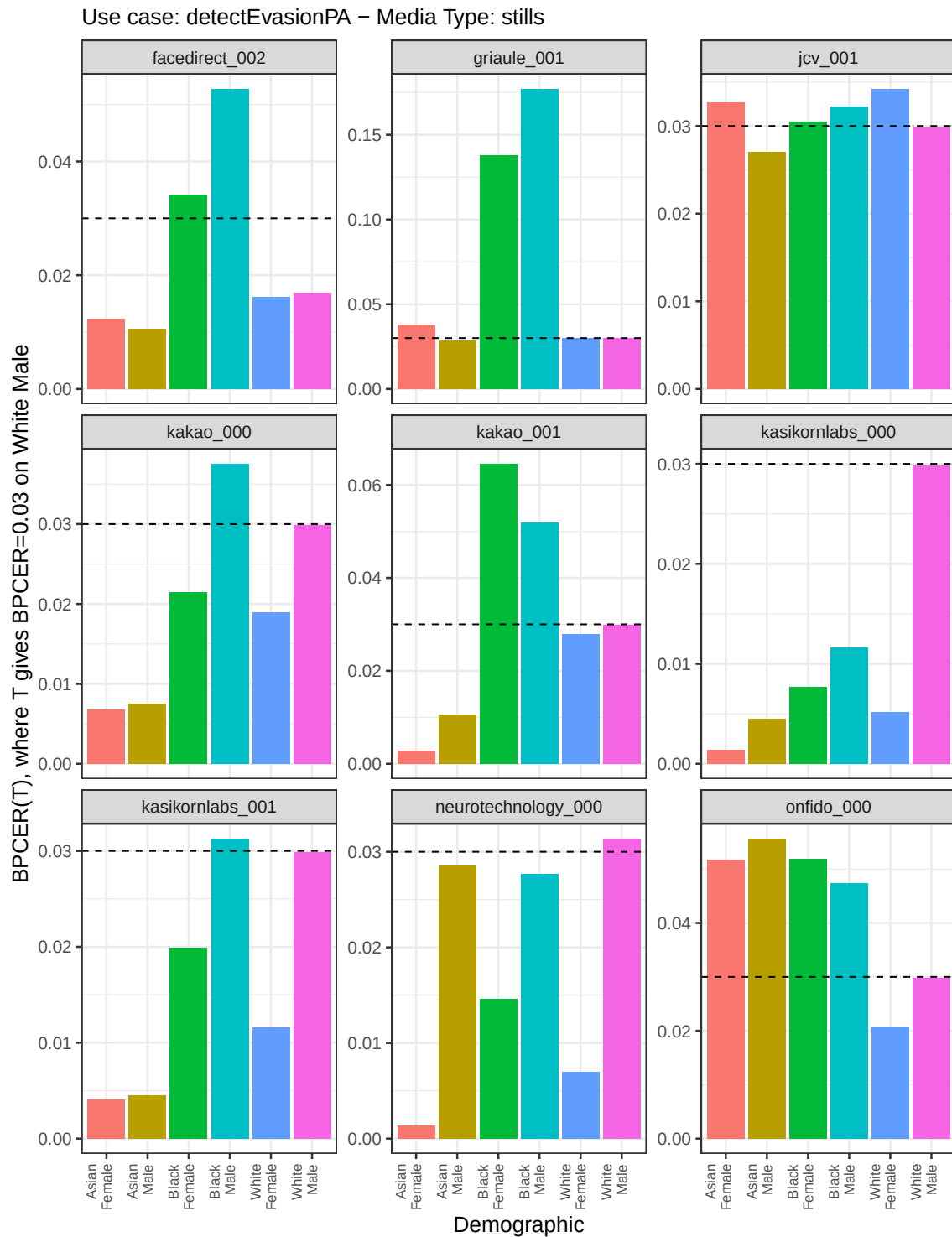
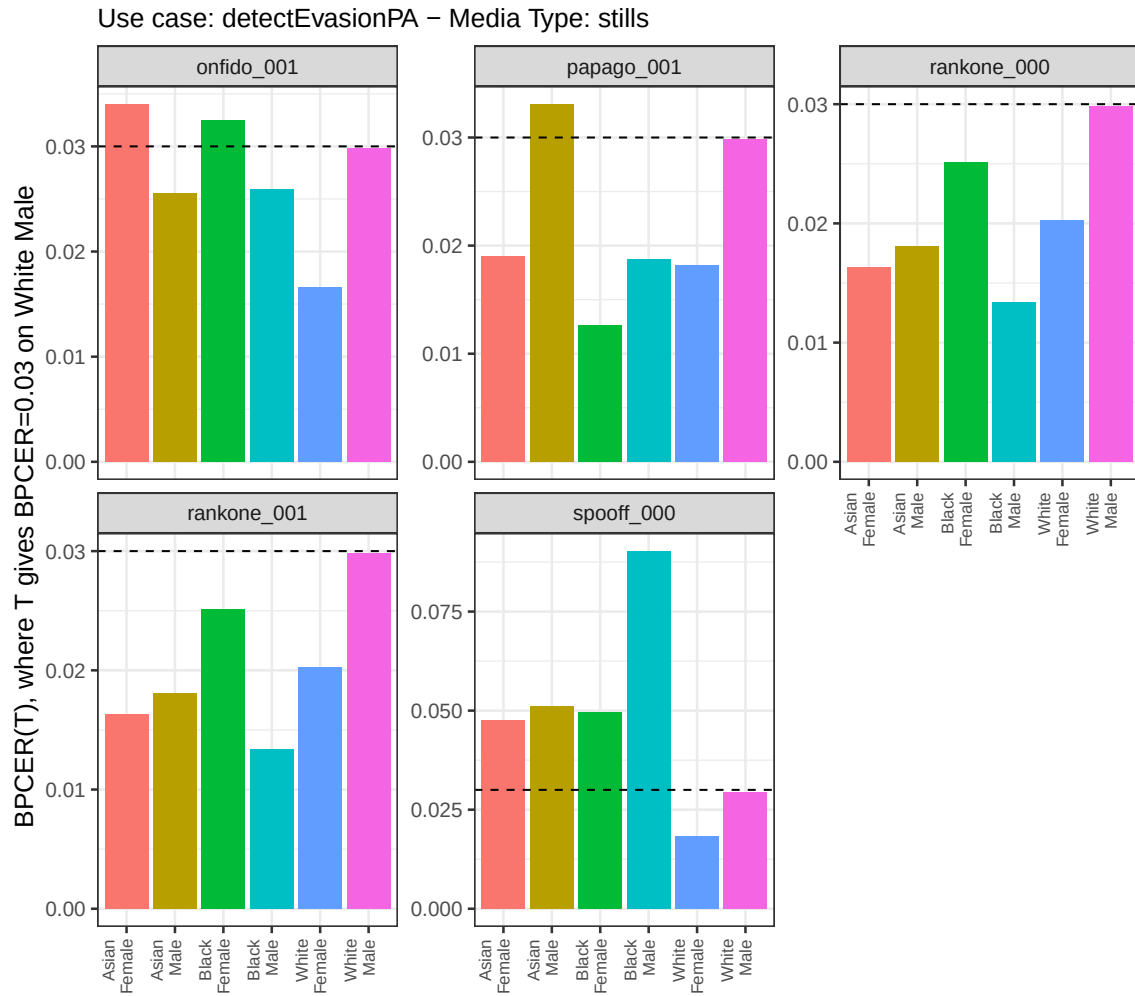


Fig. 72. The plot presents BPCER/false detection rate for different race-sex groups at a fixed threshold that gives BPCER equal (or closest) to 0.03 on White Male. Algorithms where BPCER of 0.03 is not attainable are not plotted.



Appendix D. Abbreviations

PA Presentation Attack.

PAI Presentation Attack Instrument.

PAD Presentation Attack Detection.

APCER Attack Presentation Classification Error Rate.

BPCER Bona Fide Classification Error Rate.

APNRR Attack Presentation Non-Response Rate.

BPNNR Bona Fide Presentation Non-Response Rate.