Face Anti-Spoofing for Mobile Devices

Artur Costa-Pazo

David Jiménez-Cabello

gradiant
Connectivity · Intelligence · Security
for your business

WGML
2017

(+34) 986 120 430 | gradiant@gradiant.org | www.gradiant.org

gradiant

Connectivity · Intelligence · Security

for your business

Galician Research and Development Center in Advanced Telecommunications

(+34) 986 120 430 | www.gradiant.org

Team

iNetS

Intelligent Networked Systems

eHealth

Com

Advanced Communications

S&A

Services & Applications

Team

iNetS

Intelligent Networked Systems

eHealth

Com

Advanced Communications

S&A

Services & Applications

Team

iNetS

Intelligent Networked Systems

eHealth

Com

Advanced Communications

S&A

Services & Applications

Team

MM

Multimodal Information

iNetS

Intelligent Networked Systems

Com

Advanced Communications

eHealth

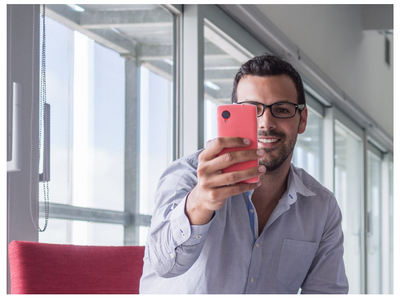
S&A

Services & Applications

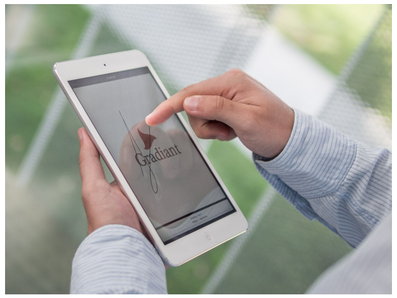
Biometrics

What modalities we work on?

Gradiant Face



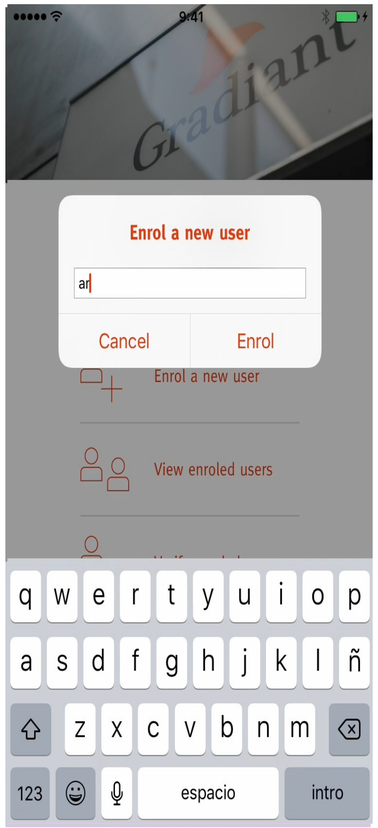
Gradiant Signature



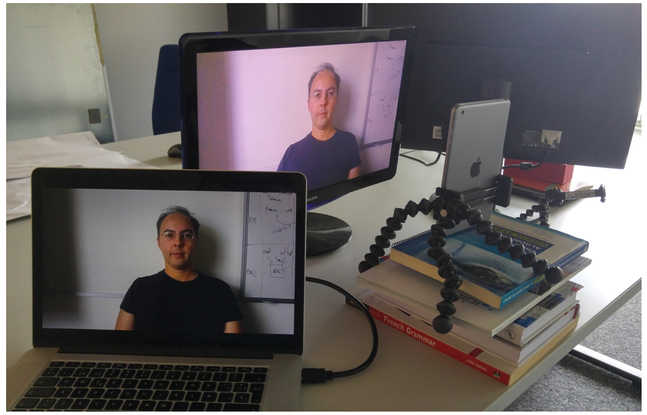
Gradiant Voice

Use case: Onboarding

Use case: Onboarding

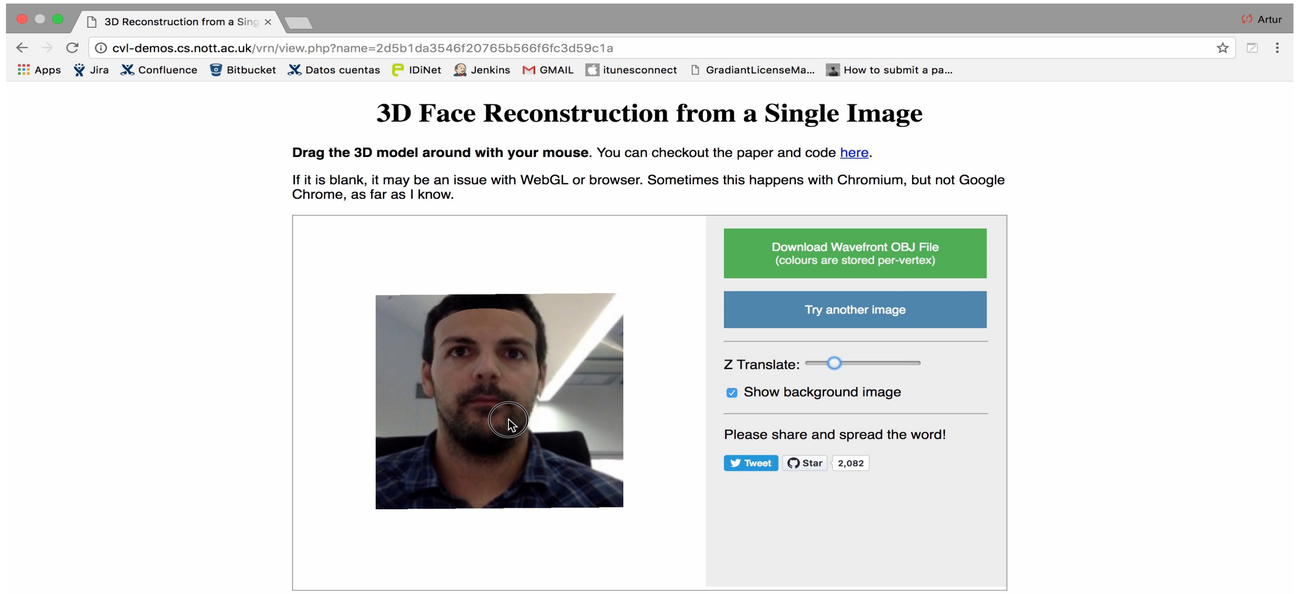


Attacks



Attacks

Attacks



http://cvl-demos.cs.nott.ac.uk/vrn/

Presentation Attack Detection (PAD)

Quality-based face-PAD

- Moire Patterns [1]
- IQM [2]

Presentation Attack Detection (PAD)

Quality-based face-PAD

- Moire Patterns [1]
- IQM [2]

Motion-based face-PAD

- Dynamic Mode Decomposition (DMD) [3]
- Optical Flow [4]
- LBP-TOP [5]

Presentation Attack Detection (PAD)

Quality-based face-PAD

- Moire Patterns [1]
- IQM [2]

Motion-based face-PAD

- Dynamic Mode Decomposition (DMD) [3]
- Optical Flow [4]
- LBP-TOP [5]

Texture-based face-PAD

- LBP [6]
- Gabor [7] **(ours)**

Presentation Attack Detection (PAD)

Quality-based face-PAD

- Moire Patterns [1]
- IQM [2]

Motion-based face-PAD

- Dynamic Mode Decomposition (DMD) [3]
- Optical Flow [4]
- LBP-TOP [5]

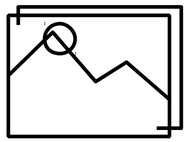
Texture-based face-PAD

- LBP [6]
- Gabor [7] **(ours)**

Others

- Survey [8]
- Challenge-response

Trending topic



Databases

- NUAA [9] (2010)
- CASIA FASD [10] (2012)
- REPLAY-ATTACK [11] (2012)
- MSU MFSD [12] (2015)
- REPLAY-MOBILE [13] (2016) (**ours)**
- OULU NPU [14] (2017)

Competitions

- ICB 2011 [15] (6 participants)
- ICB 2013 [16] (8 participants)
- IJCB 2017 [17] (14 participants)

Competition

IJCB 2017 competition on generalized face presentation attack detection in mobile authentication scenarios.

4950	14	10	4
Videos	Participants	Countries	Evaluation Protocols

Real | Print 1 | Print 2 | Replay 1 | Replay 2

www.gradiant.org

Teams

Team	Affiliations
Baseline	University of Oulu, Finland
MBLPQ	University of Ouargla, Algeria
PML	University of Biskra, Algeria University of the Basque Country, Spain University of Valenciennes, France
Massy_HNU	Hunan University, China University of Science and Technology, China
MFT-FAS	Indian Institute of Technology Indore, India
GRADIANT	Galician Research and Development Center in Advanced Telecommunications, Spain
Idiap	Ecole Polytechnique Federale de Lausanne Idiap Research Institute, Switzerland
VSS	Vologda State University, Russia
SZUCVI	Shenzhen University, China.
MixedFasNet	FUJITSU laboratories LTD, Japan
NWPU	Northwestern Polytechnical University, China
HKBU	Hong Kong Baptist University, China
Recod	University of Campinas, Brazil
CPqD	CPqD, Brazil

Teams

Team	Affiliations
Baseline	University of Oulu, Finland
MBLPQ	University of Ouargla, Algeria
PML	University of Biskra, Algeria University of the Basque Country, Spain University of Valenciennes, France
Massy_HNU	Hunan University, China University of Science and Technology, China
MFT-FAS	Indian Institute of Technology Indore, India
GRADIANT	Galician Research and Development Center in Advanced Telecommunications, Spain
Idiap	Ecole Polytechnique Federale de Lausanne Idiap Research Institute, Switzerland
VSS	Vologda State University, Russia
SZUCVI	Shenzhen University, China.
MixedFasNet	FUJITSU laboratories LTD, Japan
NWPU	Northwestern Polytechnical University, China
HKBU	Hong Kong Baptist University, China
Recod	University of Campinas, Brazil
CPqD	CPqD, Brazil

Teams

	Category	Teams
HC	Hand-crafted features	Baseline, MBLPQ, PML, Massy_HNU, MFT-FAS, GRADIANT, Idiap
L	Learned features	VSS, SZCVI, MixedFASNet
H	Hybrid features	NWPU, HKBU, Recod, CPqD

Results

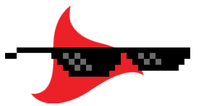
Protocol 1
(Illumination)

	Methods	Dev	Test				
		EER(%)	Video-replay	Print	Overall		
			APCER(%)	APCER(%)	APCER(%)	BPCER(%)	ACER(%)
HC	GRADIANT_extra	0.7	7.1	3.8	7.1	5.8	**6.5**
H	CPqD	0.6	1.3	2.9	2.9	10.8	6.9
HC	GRADIANT	1.1	**0.0**	1.3	1.3	12.5	6.9
H	Recod	2.2	3.3	0.8	3.3	13.3	8.3
L	MixedFASNet	1.3	**0.0**	**0.0**	**0.0**	17.5	8.8
HC	PML	0.6	7.5	11.3	11.3	9.2	10.2
HC	Baseline	4.4	5.0	1.3	5.0	20.8	12.9
HC	Massy_HNU	1.1	5.4	3.3	5.4	20.8	13.1
H	HKBU	4.3	9.6	7.1	9.6	18.3	14.0
H	NWPU	**0.0**	8.8	7.5	8.8	21.7	15.2
HC	MFT-FAS	2.2	0.4	3.3	3.3	28.3	15.8
HC	MBLPQ	2.2	31.7	44.2	44.2	**3.3**	23.8
HC	Idiap	5.6	9.6	13.3	13.3	40.0	26.7
L	VSS	12.2	20.0	12.1	20.0	41.7	30.8
L	SZUCVI	16.7	11.3	**0.0**	11.3	65.0	38.1
L	VSS_extra	24.0	9.6	11.3	11.3	73.3	42.3

Results

Protocol 2 (PAI)

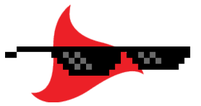
	Methods	Dev	Test				
		EER(%)	Video-replay	Print	Overall		
			APCER(%)	APCER(%)	APCER(%)	BPCER(%)	ACER(%)
HC	GRADIANT	0.9	**1.7**	3.1	**3.1**	**1.9**	**2.5**
HC	GRADIANT_extra	0.7	6.9	**1.1**	6.9	2.5	4.7
L	MixedFASNet	1.3	6.4	9.7	9.7	2.5	6.1
L	SZUCVI	4.4	3.9	3.3	3.9	9.4	6.7
HC	MFT-FAS	2.2	10.0	11.1	11.1	2.8	6.9
HC	PML	0.9	11.4	9.4	11.4	3.9	7.6
H	CPqD	2.2	9.2	14.7	14.7	3.6	9.2
L	HKBU	4.6	13.9	12.5	13.9	5.6	9.7
H	Recod	3.7	13.3	15.8	15.8	4.2	10.0
HC	MBLPQ	1.9	5.6	19.7	19.7	6.1	12.9
HC	Baseline	4.1	15.6	22.5	22.5	6.7	14.6
HC	Massy_HNU	1.3	16.1	26.1	26.1	3.9	15.0
HC	Idiap	8.7	21.7	7.5	21.7	11.1	16.4
L	NWPU	**0.0**	12.5	5.8	12.5	26.7	19.6
H	VSS	14.8	25.3	13.9	25.3	23.9	24.6
H	VSS_extra	23.3	36.1	33.9	36.1	33.1	34.6



Results

Protocol 3 (LOCO)

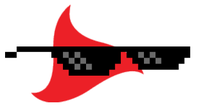
	Methods	Dev	Test				
		EER(%)	Video-replay	Print	Overall		
			APCER(%)	APCER(%)	APCER(%)	BPCER(%)	ACER(%)
HC	GRADIANT	0.9±0.4	1.0±1.7	2.6±3.9	2.6±3.9	**5.0±5.3**	**3.8±2.4**
HC	GRADIANT_extra	0.7±0.2	1.4±1.9	**1.4±2.6**	**2.4±2.8**	5.6±4.3	4.0±1.9
L	MixedFASNet	1.4±0.5	1.7±3.3	5.3±6.7	5.3±6.7	7.8±5.5	6.5±4.6
H	CPqD	0.9±0.4	4.4±3.4	5.0±6.1	6.8±5.6	8.1±6.4	7.4±3.3
H	Recod	2.9±0.7	4.2±3.8	8.6±14.3	10.1±13.9	8.9±9.3	9.5±6.7
HC	MFT-FAS	0.8±0.4	**0.8±0.9**	10.8±18.1	10.8±18.1	9.4±12.8	10.1±9.9
HC	Baseline	3.9±0.7	9.3±4.3	11.8±10.8	14.2±9.2	8.6±5.9	11.4±4.6
H	HKBU	3.8±0.3	7.9±5.8	9.9±12.3	12.8±11.0	11.4±9.0	12.1±6.5
L	SZUCVI	7.0±1.6	10.0±8.3	7.5±9.5	12.1±10.6	16.1±8.0	14.1±4.4
HC	PML	1.1±0.3	8.2±12.5	15.3±22.1	15.7±21.8	15.8±15.4	15.8±15.1
HC	Massy_HNU	1.9±0.6	5.8±5.4	19.0±26.7	19.3±26.5	14.2±13.9	16.7±10.9
HC	MBLPQ	2.3±0.6	5.8±5.8	12.9±4.1	12.9±4.1	21.9±22.4	17.4±10.3
H	NWPU	**0.0±0.0**	1.9±0.7	1.9±3.3	3.2±2.6	33.9±10.3	18.5±4.4
HC	Idiap	7.9±1.9	8.3±3.0	9.3±10.0	12.9±8.2	26.9±24.4	19.9±11.8
L	VSS	14.6±0.8	21.4±7.7	13.8±7.0	21.4±7.7	25.3±9.6	23.3±2.3
L	VSS_extra	25.9±1.7	25.0±11.4	32.2±27.9	40.3±22.2	35.3±27.4	37.8±6.8



Results

Protocol 4 (ALL)

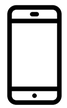
	Methods	Dev	Test				
		EER(%)	Video-replay	Print	Overall		
			APCER(%)	APCER(%)	APCER(%)	BPCER(%)	ACER(%)
HC	GRADIANT	1.1±0.3	**0.0±0.0**	5.0±4.5	5.0±4.5	15.0±7.1	**10.0±5.0**
HC	GRADIANT_extra	1.1±0.3	27.5±24.2	5.8±4.9	27.5±24.2	**3.3±4.1**	15.4±11.8
HC	Massy_HNU	1.0±0.4	20.0±17.6	26.7±37.5	35.8±35.3	8.3±4.1	22.1±17.6
H	CPqD	2.2±1.7	16.7±16.0	24.2±39.4	32.5±37.5	11.7±12.1	22.1±20.8
H	Recod	3.7±0.7	20.0±19.5	23.3±40.0	35.0±37.5	10.0±4.5	22.5±18.2
HC	MFT-FAS	1.6±0.7	**0.0±0.0**	12.5±12.9	12.5±12.9	33.3±23.6	22.9±8.3
L	MixedFASNet	2.8±1.1	10.0±7.7	4.2±4.9	10.0±7.7	35.8±26.7	22.9±15.2
HC	Baseline	4.7±0.6	19.2±17.4	22.5±38.3	29.2±37.5	23.3±13.3	26.3±16.9
H	HKBU	5.0±0.7	16.7±24.8	21.7±36.7	33.3±37.9	27.5±20.4	30.4±20.8
L	VSS	11.8±0.8	21.7±8.2	9.2±5.8	21.7±8.2	44.2±11.1	32.9±5.8
HC	MBLPQ	3.6±0.7	35.0±25.5	45.0±25.9	49.2±27.8	24.2±27.8	36.7±4.7
H	NWPU	**0.0±0.0**	30.8±7.4	6.7±11.7	30.8±7.4	44.2±23.3	37.5±9.4
HC	PML	0.8±0.3	59.2±24.2	38.3±41.7	61.7±26.4	13.3±13.7	37.5±14.1
L	SZUCVI	9.1±1.6	**0.0±0.0**	**0.8±2.0**	**0.8±2.0**	80.8±28.5	40.8±13.5
HC	Idiap	6.8±0.8	26.7±35.2	13.3±8.2	33.3±30.4	54.2±12.0	43.8±20.4
L	VSS_extra	21.1±2.7	13.3±17.2	15.8±21.3	25.8±20.8	70.0±22.8	47.9±12.1



Results

https://sites.google.com/site/faceantispoofing/results

Our method



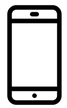
Capture

Features extraction

Dimensionality reduction

Classifier

Our method



Capture

Load from file

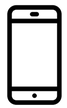
Access to native camera

Features extraction

Dimensionality reduction

Classifier

Our method



Capture

Load from file

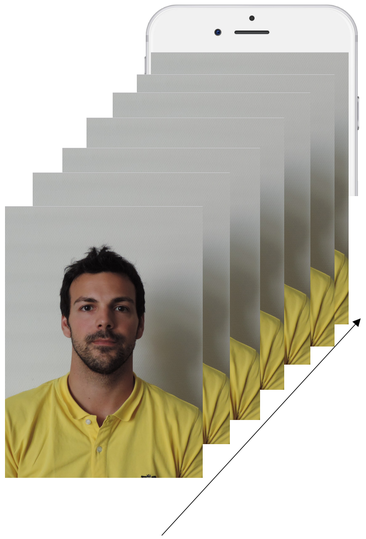
Access to native camera

Features extraction

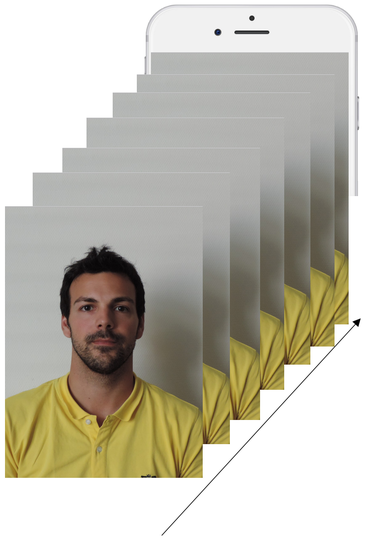
Dimensionality reduction

Classifier

Features Extractor



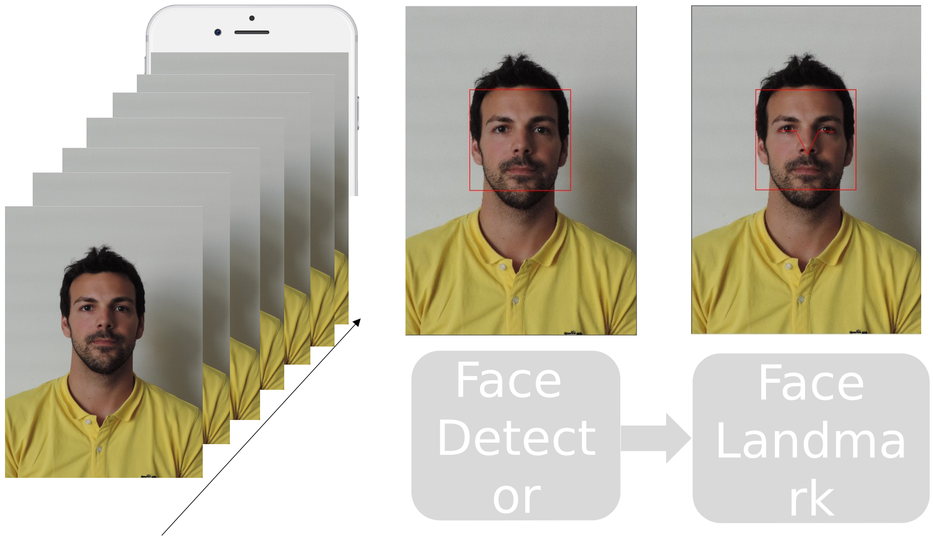
Features Extractor



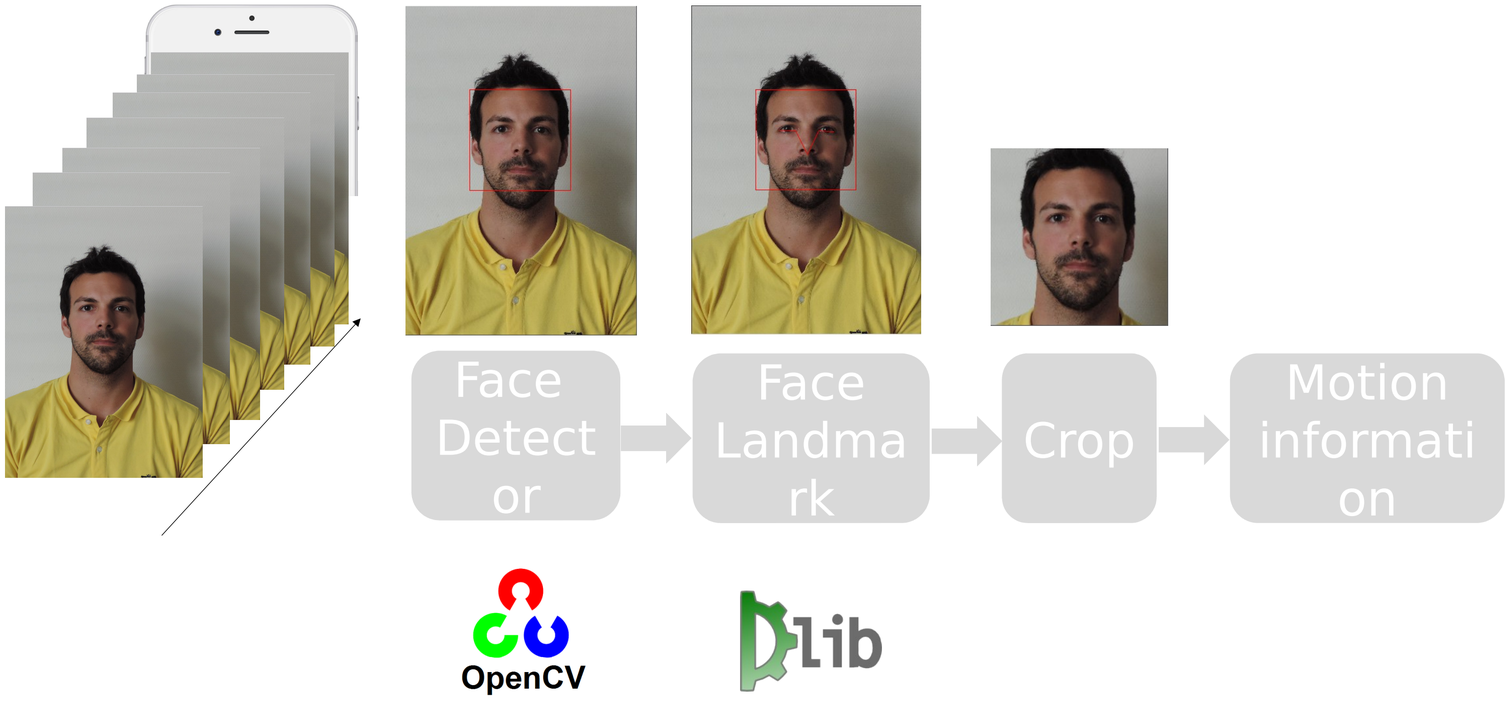
Face Detect or

OpenCV

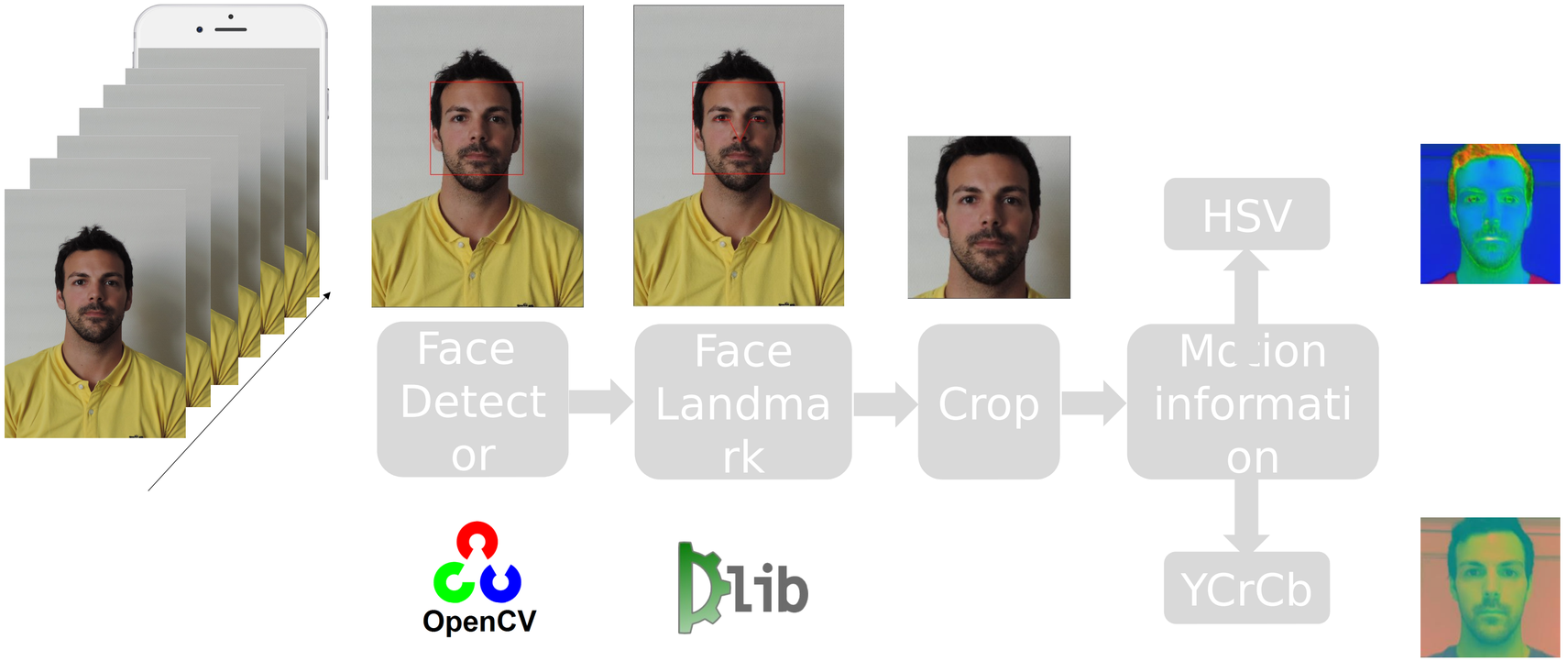
Features Extractor



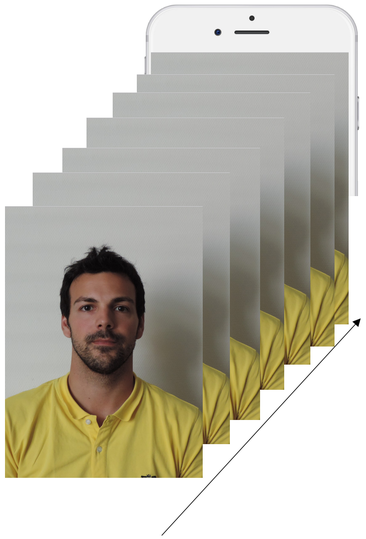
Features Extractor



Features Extractor



Features Extractor



Face Detector

Face Landmark

Crop

Motion information

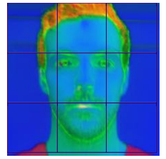
HSV

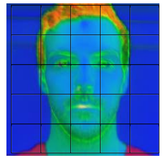
YCrCb

OpenCV

Dlib

LBP
Blocks 3x3 and 5x5

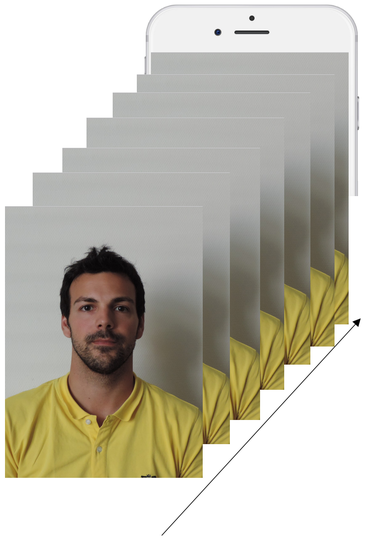




6018-length vector

6018-length vector

Features Extractor



Our method

Capture

Load from file

Access to native camera

Features extraction

6018-length feature vector. HSV

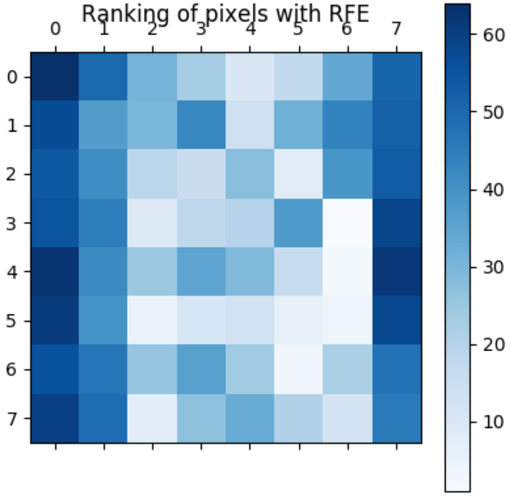
6018-length feature vector. YCrCb

Dimensionality reduction

Classifier

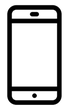
Recursive feature elimination

From two 6018-length feature vectors to two 1000-length feature vectors.



http://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.RFE.html

Our method



Capture

Load from file

Access to native camera

Features extraction

6018-length feature vector. HSV

6018-length feature vector. YCrCb

Dimensionality reduction

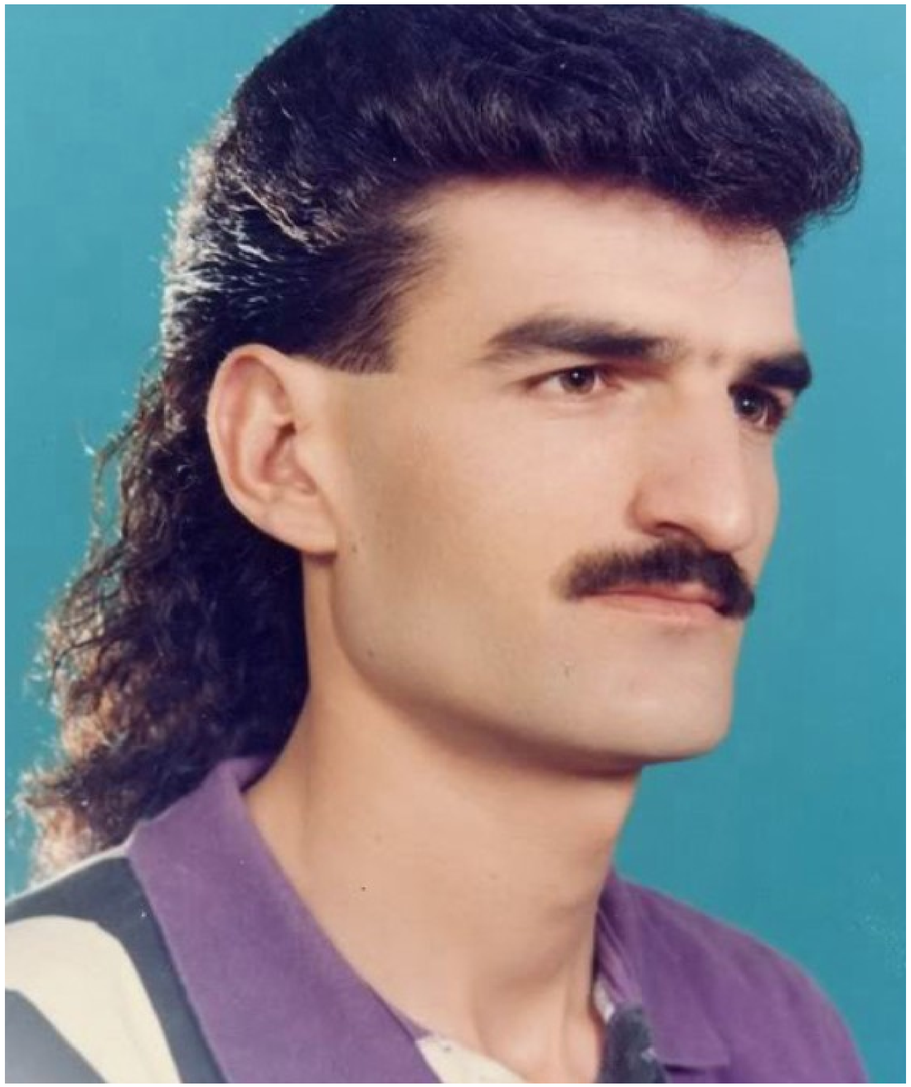
1000-length feature vector. HSV

1000-length feature vector. YCrCb

Classifier

Classifier

SVM. Kernel RBF



Oldie but goldie

Our method

Capture

Load from file

Access to native camera

Features extraction

6018-length feature vector. HSV

6018-length feature vector. YCrCb

Dimensionality reduction

1000-length feature vector. HSV

1000-length feature vector. YCrCb

Classifier

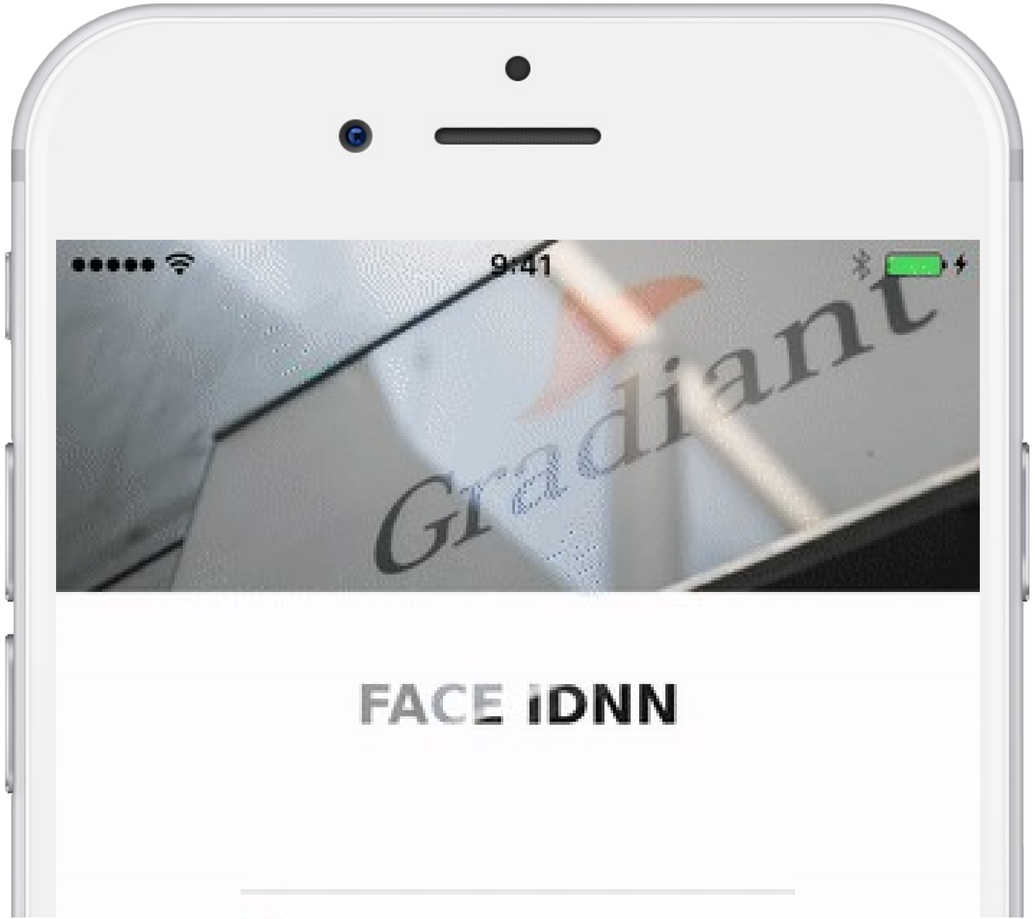
SVM-RBF

Score Fusion

Future work

Train CNNs

Release a version



Novel evaluation protocols

(New publication)

Ask your questions

www.gradiant.org

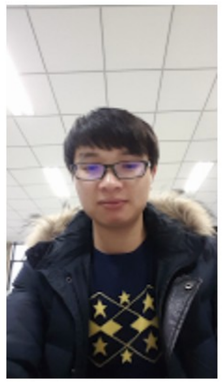
Thank you ^

+ info in the appendix

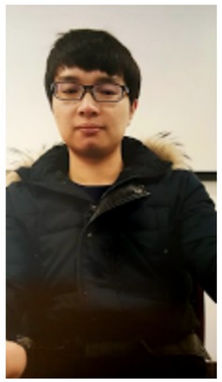
(+34) 986 120 430 | gradiant@gradiant.org | www.gradiant.org

Appendix

Competition Database


Real


Print 1


Print 2


Replay 1


Replay 2

	Users	Real access	Print attacks	Video attacks	Total
Training	20	360	720	720	1800
Development	15	270	540	540	1350
Test	20	360	720	720	1800

6 Devices: Samsung Galaxy S6 edge, HTC Desire EYE, MEIZU X5, ASUS Zenfone Selfie, Sony XPERIA C5 Ultra Dual and OPPO N3

Evaluation Protocols

Protocol I: The first protocol is designed to evaluate the generalization of the face PAD methods under previously unseen environmental conditions, namely **illumination** and background scene. As the database is recorded in three sessions with different illumination condition and location, the train, development and evaluation sets are constructed using video recordings taken in different sessions.

Protocol II: The second protocol is designed to evaluate the effect of attacks created with **different printers or displays** on the performance of the face PAD methods as they may suffer from new kinds of artifacts. The effect of attack variation is assessed by introducing a previously unseen print and video-replay attack in the test set.

Protocol III: One of the critical issues in face PAD and image classification in general is **sensor** interoperability. To study the effect of the input camera variation, a Leave One Camera Out (**LOCO**) protocol is used. In each iteration, the real and the attack videos recorded with five smartphones are used to train and tune the algorithms, and the generalization of the models is assessed using the videos recorded with the remaining one.

Protocol IV: In the last and most challenging protocol, all above three factors are considered simultaneously and generalization of face PAD methods are evaluated across previously unseen environmental conditions, attacks and input sensors.

Measures (PAD)

- **EER: Equal Error Rate**

Measures (PAD)

EER: Equal Error Rate

HTER: Half Total Error Rate

e.g Tune your face-PAD system on the EER of the development set and use this threshold to find the HTER on the test set scores.

Measures (PAD)

EER: Equal Error Rate

HTER: Half Total Error Rate

e.g Tune your face-PAD system on the EER of the development set and use this threshold to find the HTER on the test set scores.

ACER: Average Classification Error Rate

$ACER = (APCER + BPCER)/2$

APCER: Attack Presentation Classification Error Rate; and BPCER: Bona fide Presentation Classification Error Rate.

Standard ISO/IEC 30107-3 metrics

Measures (PAD)

EER: Equal Error Rate

HTER: Half Total Error Rate

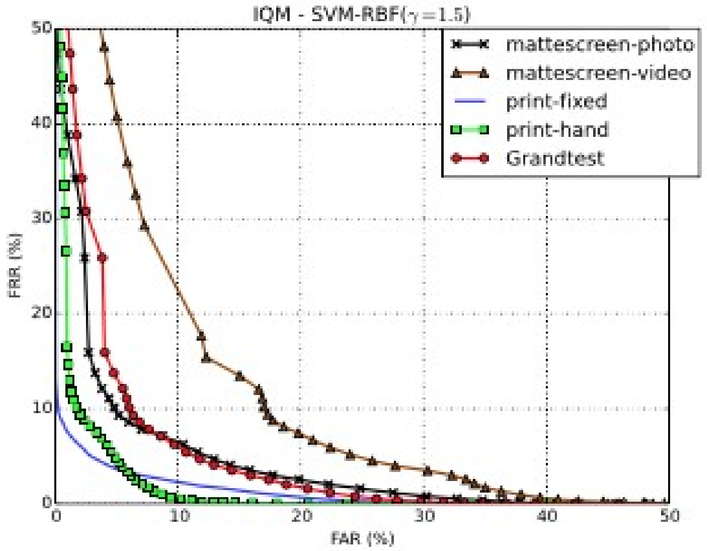
e.g Tune your face-PAD system on the EER of the development set and use this threshold to find the HTER on the test set scores.

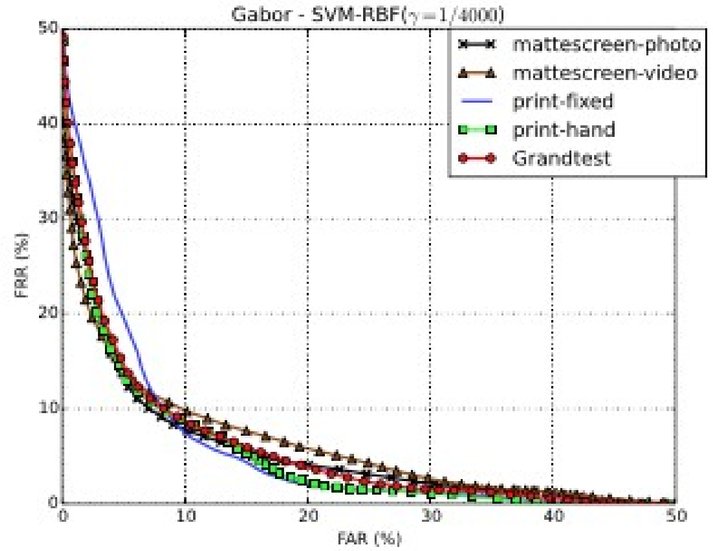
ACER: Average Classification Error Rate

ACER = (APCER + BPCER)/2

APCER: Attack Presentation Classification Error Rate; and BPCER: Bona fide Presentation Classification Error Rate.

Standard ISO/IEC 30107-3 metrics





	Test. HTER (%)					Test. ACER (%)	Test. APCER (%)	Test. BPCER (%)
	MP	MV	PF	PH	GT			
IQM	7.70	13.64	4.22	5.43	7.80	13.64	19.87	7.40
Gabor	8.64	9.53	9.40	8.99	9.13	**9.53**	7.91	11.15

Comparison of two face-PAD methods on REPLAY-MOBILE.

Muchas Gracias ^

(+34) 986 120 430 | gradiant@gradiant.org | www.gradiant.org

Contact me

Artur Costa-Pazo

Software Engineer & PhD Student

acosta@gradiant.org