Impact of facial beautification on face recognition:

From plastic surgery to makeup presentation attacks

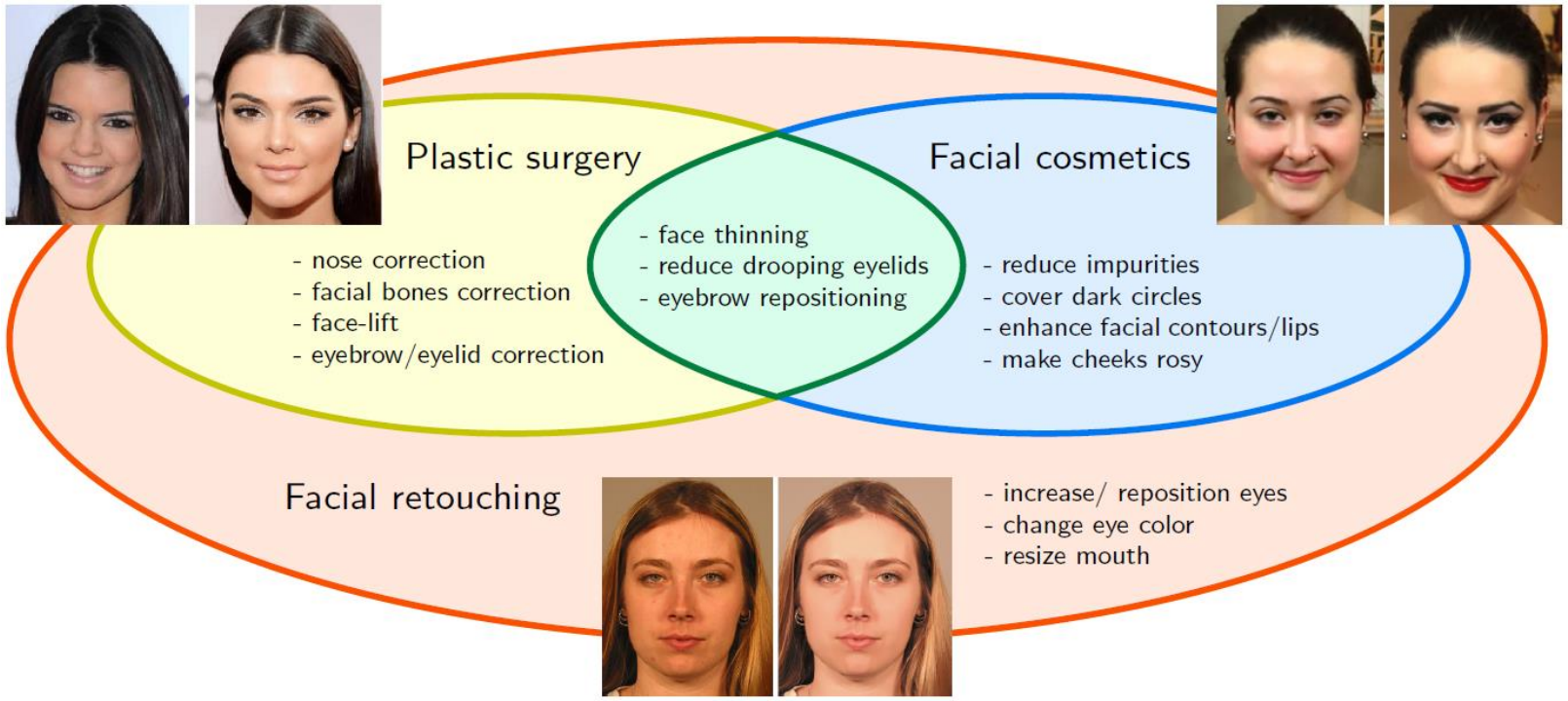
Christian Rathgeb

Hochschule Darmstadt, ATHENE, da/sec Security Research Group

International Face Performance Conference (IFPC), 28.10.2020

1. Introduction
2. Plastic Surgery
3. Retouching
4. Makeup
5. Makeup Presentation Attack Detection

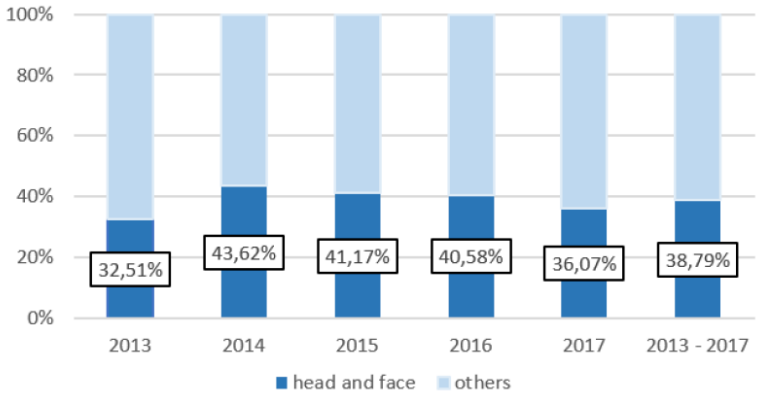
Facial Beautification and Detection



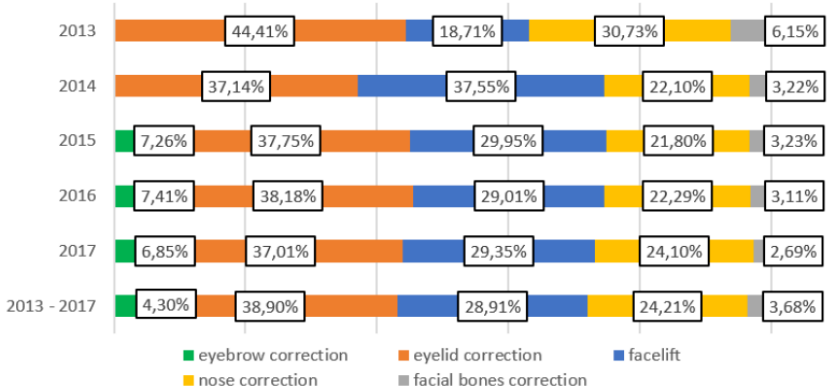
- Scenario: either the reference or the probe image has been altered
- Further types of beautification: tattoos, piercings, etc.

Christian Rathgeb, Antitza Dantcheva, Christoph Busch, „Impact and Detection of Facial Beautification in Face Recognition: An Overview“, in *IEEE Access*, 7(1), 2019.

Plastic Surgery

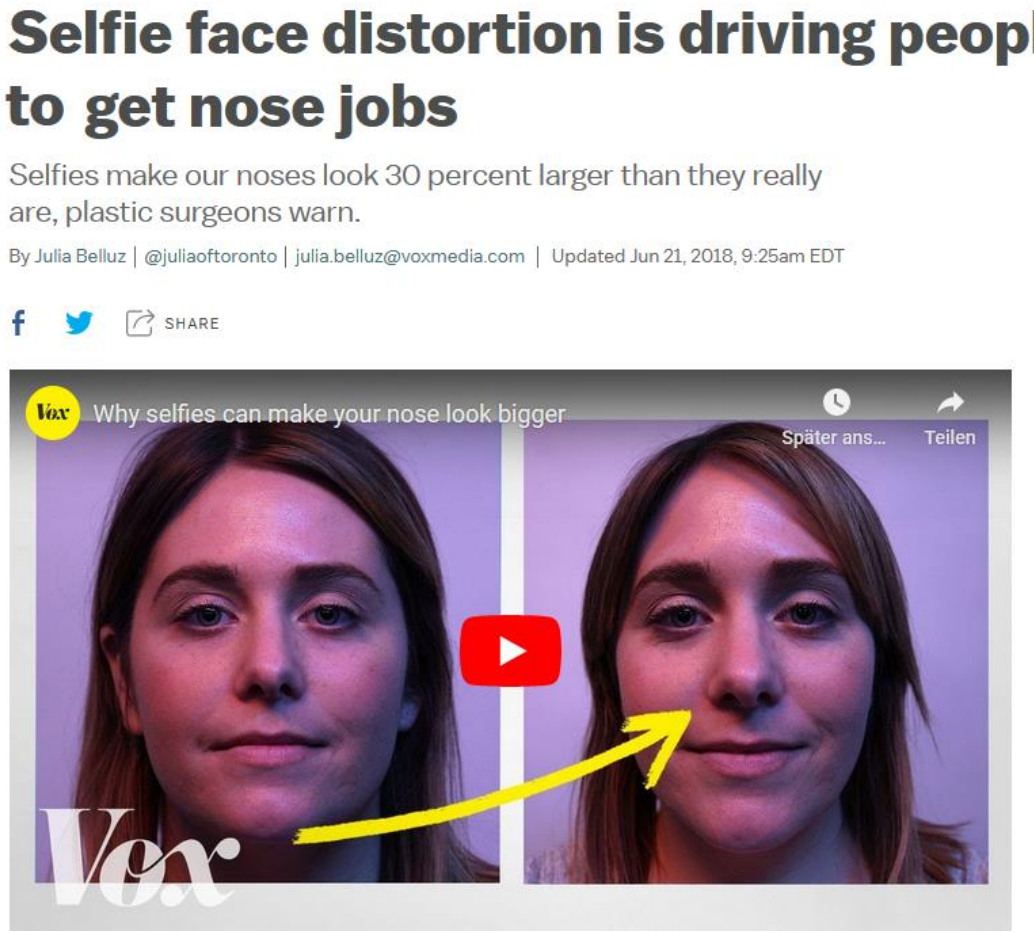


(a) head and face plastic surgeries



(b) types of plastic surgeries on head and face

Source: International Society of Aesthetic Plastic Surgery



Selfie face distortion is driving people to get nose jobs

Selfies make our noses look 30 percent larger than they really are, plastic surgeons warn.

By Julia Belluz | @juliaoftoronto | julia.belluz@voxmedia.com | Updated Jun 21, 2018, 9:25am EDT

SHARE

Plastic Surgery

(a) unaltered (b) eyebrow correction (c) eyelid correction

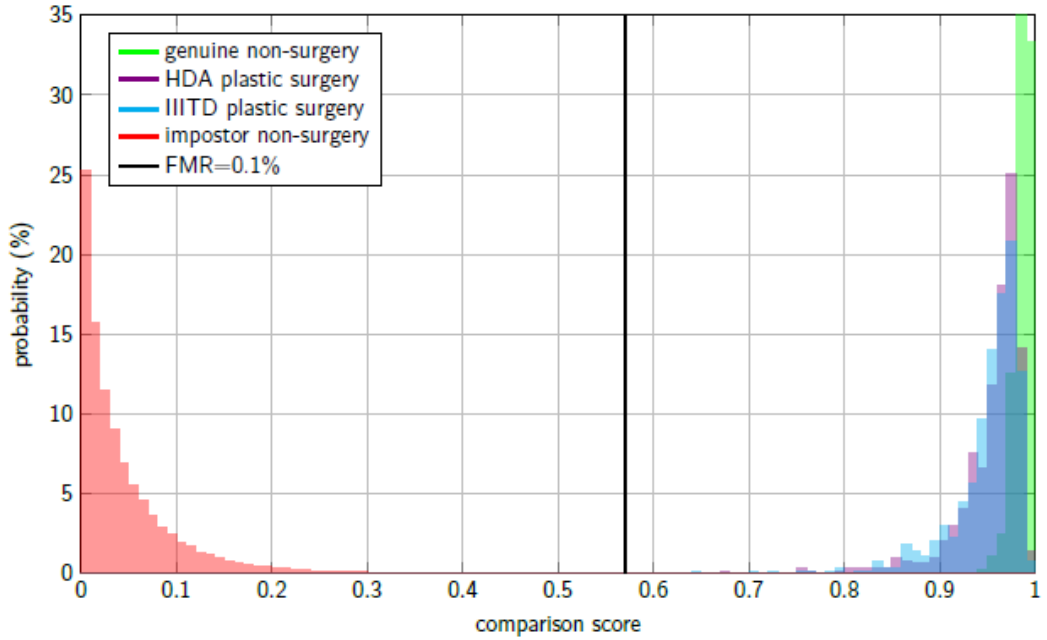
(d) facelift (e) nose correction (f) facial bones correction

Database	Surgery	Image pairs	
		Genuine	Impostor
IIITD plastic surgery	Dermabrasion	32	–
	Eyebrow correction	60	–
	Ear correction	74	–
	Eyelid correction	105	–
	Nose correction	192	–
	Skin peeling	73	–
	Facelift	308	–
	Others (mentoplasty, etc.)	56	–
HDA plastic surgery	Eyebrow correction	128	–
	Eyelid correction	131	–
	Facelift	98	–
	Nose correction	174	–
	Facial bones correction	107	–
Non-surgery	Non	900	404,550

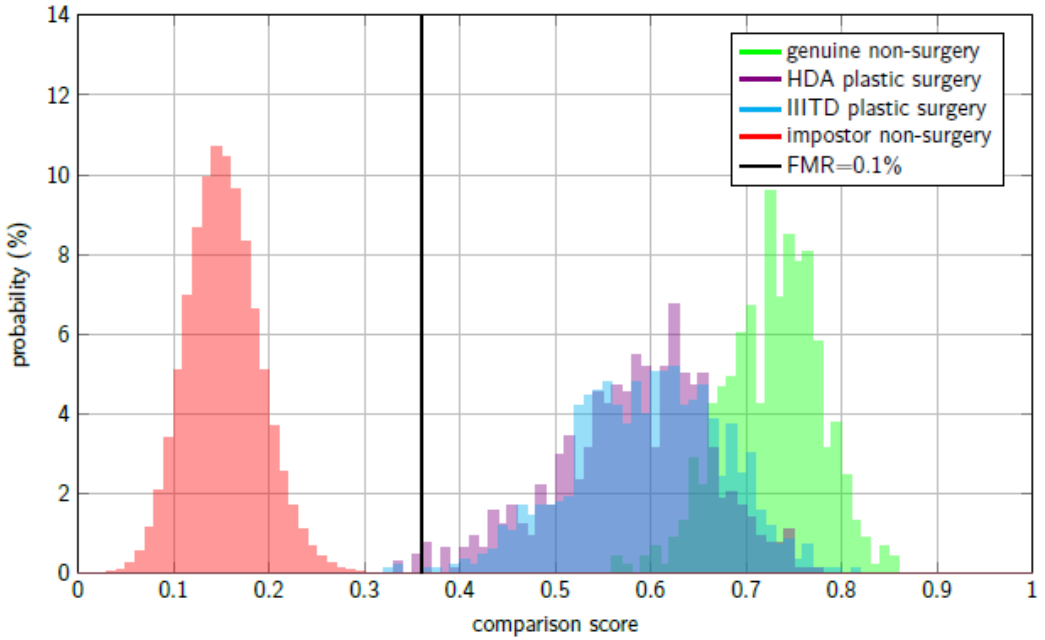
- Verification with ArcFace and Cognitec

Christian Rathgeb, Didem Dogan, Fabian Stockhardt, Maria De Marsico, Christoph Busch, „Plastic Surgery: An Obstacle for Deep Face Recognition?“, in *15th IEEE Computer Society Workshop on Biometrics (CVPRW)*, 2020.

Plastic Surgery



(a) Cognitec FaceVACS



(b) ArcFace

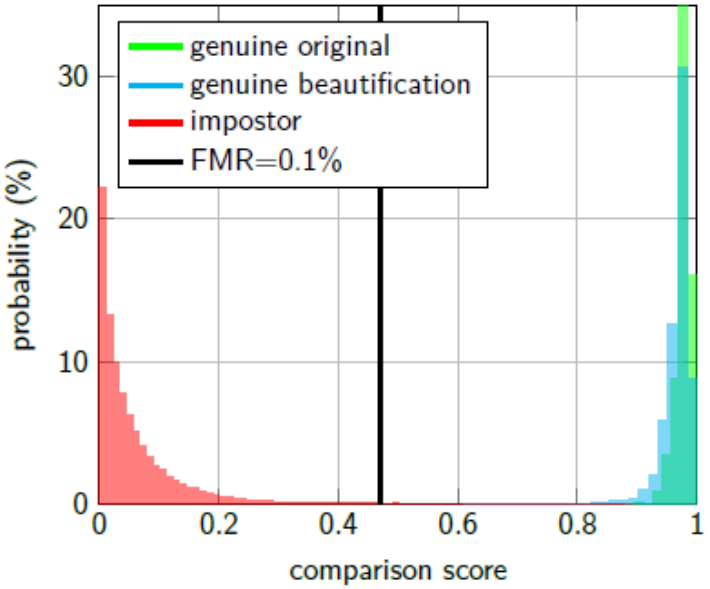
- Low impact on biometric performance
- Only in case of severe alterations, e.g. feminisation sugeries

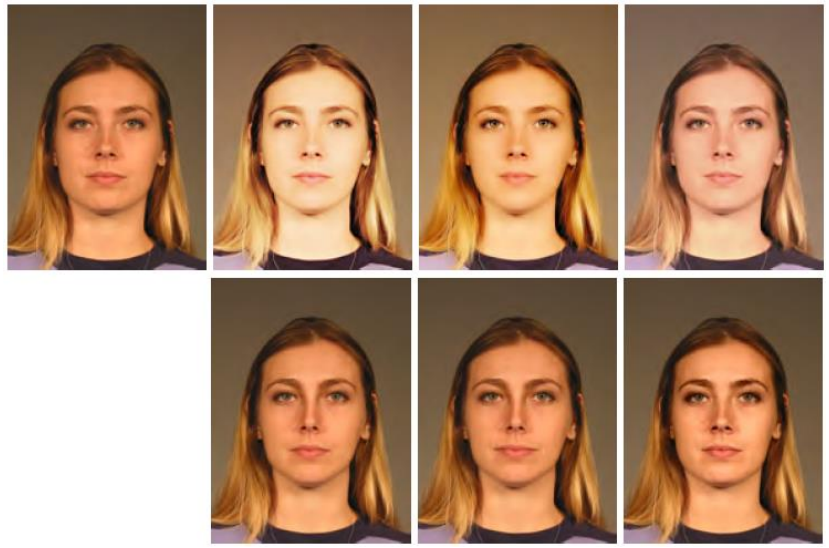
Retouching

- Users may apply retouching with easy-to-use apps
- Common alterations: smoothing skin, slimming nose, enlargeing eyes

Retouching

- Evaluation with Cognitec shows negligible impact on biometric performance
- Detection of retouching of interest





These two Ralph Lauren images feature the same model, Filippa Hamilton. The image on the left drew heavy criticism for its alteration to impossible body proportions.

Christian Rathgeb, Angelika Botaljov, Fabian Stockhardt, Sergey Isadskiy, Luca Debiasi, Andreas Uhl, Christoph Busch, „PRNU-based Detection of Facial Retouching“, in *IET-Biometrics*, 2020.
Christian Rathgeb, Claudia-Ioana Satnoianu, Nathania E. Haryanto, Kevin Bernardo, Christoph Busch, „Differential Detection of Facial Retouching: A Multi-Biometric Approach“, in *IEEE Access*, 2020.

Makeup

(a) makeup (taken from YMU) (b) digital makeup using ModiFace (c) GAN-based makeup transfer by Chang *et al.*

- Cost-efficient way for beautification (mostly applied by women)
- Areas: lips, skin, eyes
- Alteration of percieved anatomy

Antitza Dantcheva, Cunjian Chen, Arun Ross, „Can facial cosmetics affect the matching accuracy of face recognition systems? “, in *IEEE Fifth international conference on biometrics: theory, applications and systems (BTAS)*, 2012.

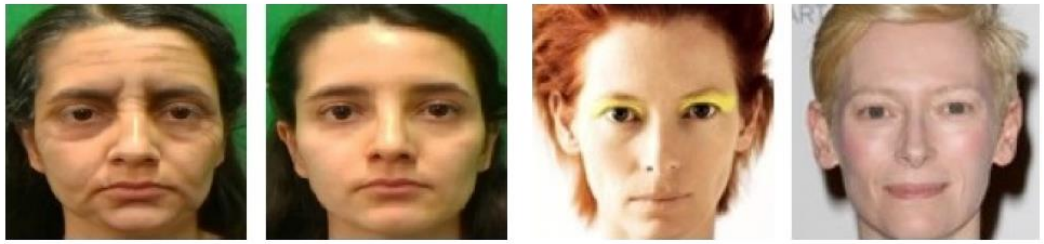
Makeup Presentation Attacks

- Impact on face recognition in case of severe alterations

(a) Before (b) After (c) Target

Public databases containing makeup presentation attacks:

(a) MIFS (b) DFW



(c) AIM (d) DMFaces

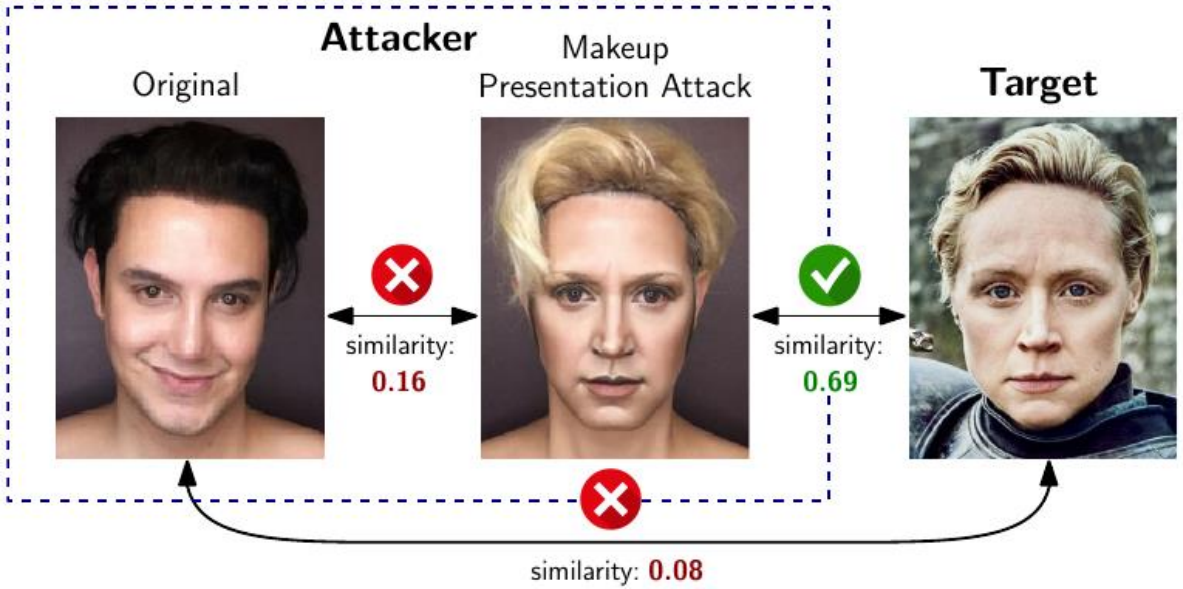
Table 1 — Examples of artificial and human presentation attack instruments

Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up

Source: ISO/IEC 30107-1:2016(E)

Makeup Presentation Attacks

- Attacker may apply makeup for impersonation or concealment
- Detection is difficult since bona fide users may also apply makeup



PAI	PAD Analysis: Image, Video	Motion	Depth	Multi-spectral	Thermal	Light-field	Challenge response
Printout	✓	✓	✓	✓	✓	✓	✓
Image on display	✓	✓	✓	✓	✓	✓	✓
Video on display	✓		✓	✓	✓	✓	✓
3D printout	✓	✓		✓	✓		✓
3D paper mask	✓			✓	✓		
3D silicone mask	✓			✓	✓		
Makeup	✓		(✓)				

Cunjian Chen, Antitza Dantcheva, Thomas Swearingen, Arun Ross, "Spoofing Faces Using Makeup: An Investigative Study," in *Proc. of 3rd IEEE Int. Conf. on Identity, Security and Behavior Analysis (ISBA)*, 2017.
Christian Rathgeb, Pawel Drozdowski, Daniel Fischer, Christoph Busch, “Vulnerability Assessment and Detection of Makeup Presentation Attacks,” in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, 2020.

Makeup Presentation Attacks

- Vulnerability analysis using Cognitec and ArcFace
- Use of MIFS/DFW databases for attacks and FRGCv2 for bona fide
- High Impostor Attack Presentation Match Rates (IAPMR) and Relative Impostor Attack Presentation Accept Rates (RIAPAR)

System	FMR	FNMR	IAPMR		RIAPAR	
			MIFS	DFW	MIFS	DFW
COTS	0.001	2.085	0.000	1.121	2.085	3.206
	0.010	0.751	1.878	4.746	2.629	5.497
	0.100	0.500	6.573	14.898	7.073	15.398
	1.000	0.334	29.577	44.034	29.911	44.368
ArcFace	0.001	1.090	1.168	2.742	2.258	3.832
	0.010	0.922	2.804	7.759	3.726	8.681
	0.100	0.838	7.243	21.940	8.081	22.778
	1.000	0.587	32.477	51.104	33.063	51.691

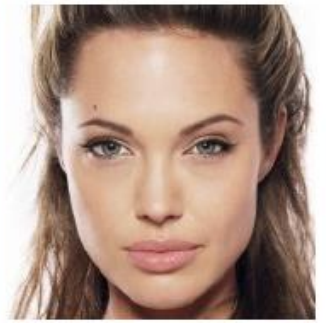
(a) before

(b) after

(c) target

(a) before

(b) after

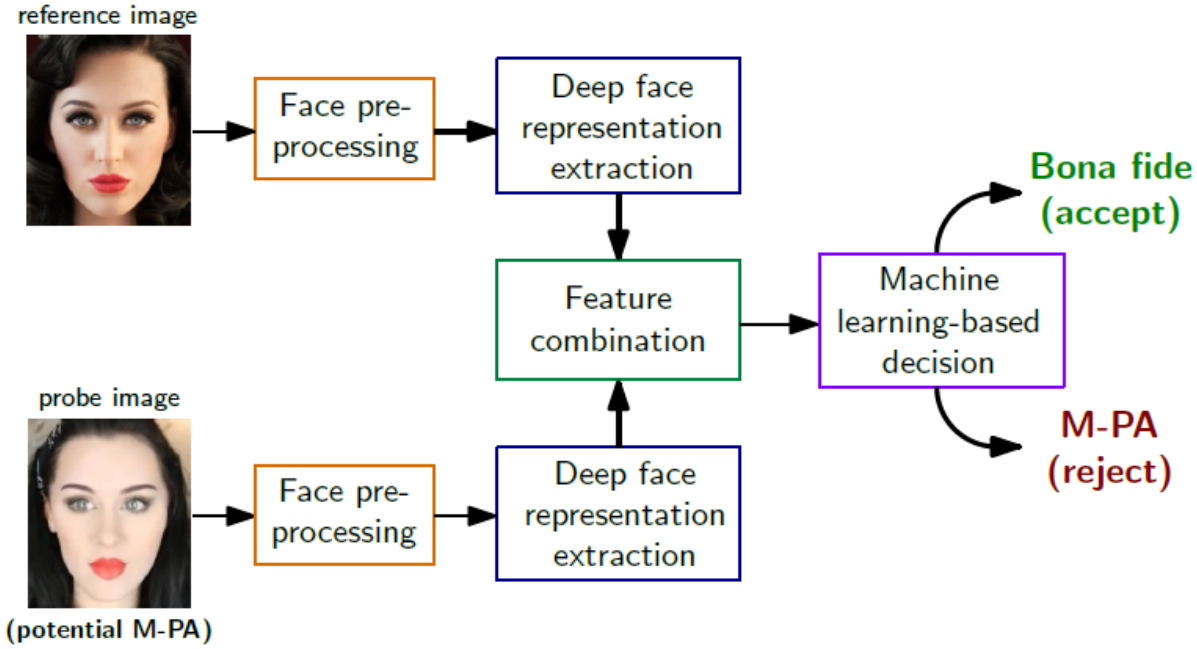


(c) target

Makeup Presentation Attacks

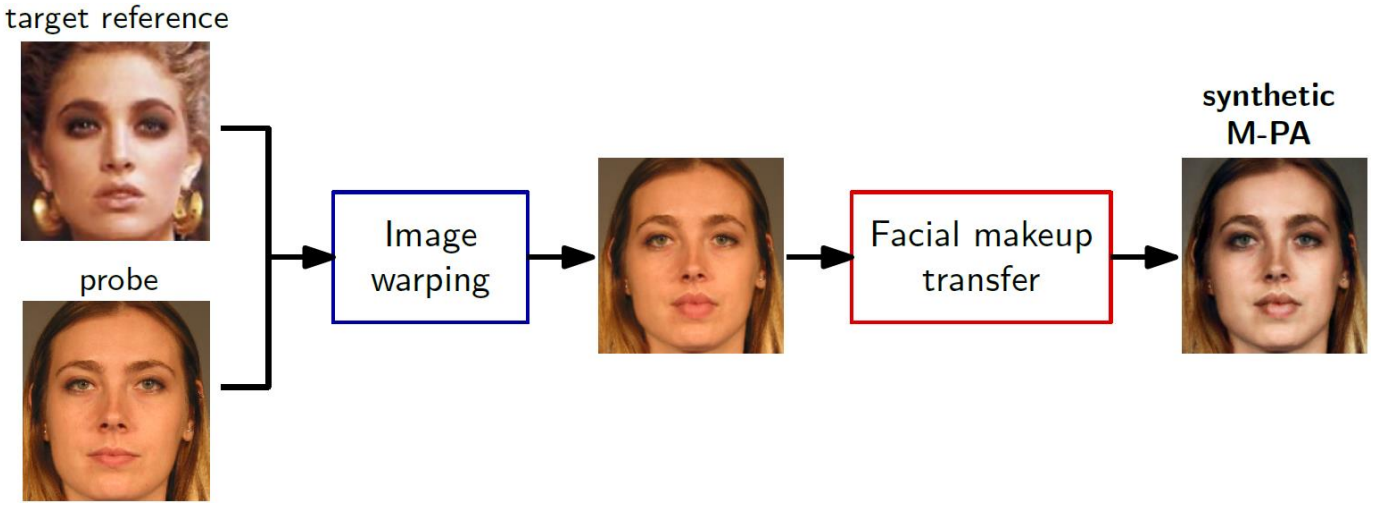
- Detection of attack in a differential detection scenario employ deep face representations
- Classification with SVM

- **Problem**: missing training data
- **Idea**: create a semi-synthetic database of makeup presentation attacks



Christian Rathgeb, Pawel Drozdowski, Christoph Busch, „Detection of Makeup Presentation Attacks based on Deep Face Representations“, in *25th International Conference on Pattern Recognition (ICPR)*, 2020.

Makeup Presentation Attacks

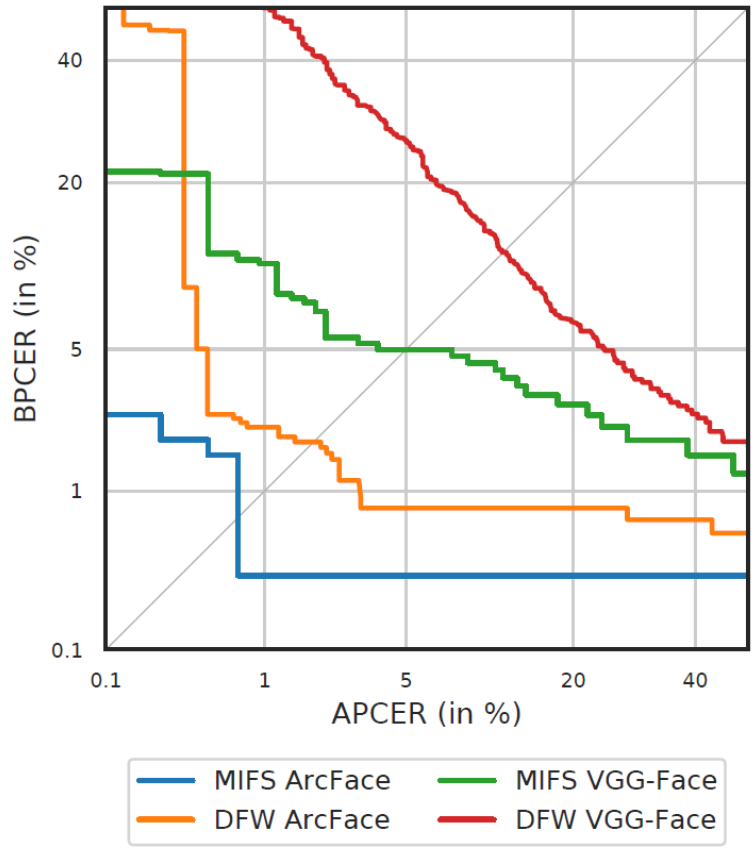


- Combination of image warping and makeup style transfer
- Target subjects from CelebA database

Makeup Presentation Attacks

- Good performance using ArcFace for feature extraction (in a differential scenario)
- D-EER: APCER=BPCER
- BPCER10: APCER=10%
- BPCER20: APCER=5%

Feature Type	Mode	Feature Extractor	D-EER		BPCER10		BPCER20	
			MIFS	DFW	MIFS	DFW	MIFS	DFW
DFR	single-image	ArcFace	38.785	44.860	83.652	89.953	90.068	92.991
FL	differential	dlib	19.484	40.768	28.125	78.132	45.313	87.813
FL	differential	OpenCV	25.837	41.116	43.770	76.257	52.716	86.433
TD	differential	LBP	33.803	45.168	93.569	86.023	97.917	91.250
TD	differential	BSIF	30.986	42.341	49.063	85.795	59.375	91.705
DFR	differential	VGG-Face	4.984	11.824	4.361	15.040	4.984	26.177
DFR	differential	ArcFace	0.704	1.791	0.313	0.799	0.313	0.799



Thank you for your attention!

Questions?