WIFS 2023

Reversing Deep Face Embeddings with Probable Privacy Protection

Dailé Osorio-Roig, Paul A. Gerlitz, Christian Rathgeb, and Christoph Busch

da/sec – Biometrics and Security Research Group

Hochschule Darmstadt

Agenda

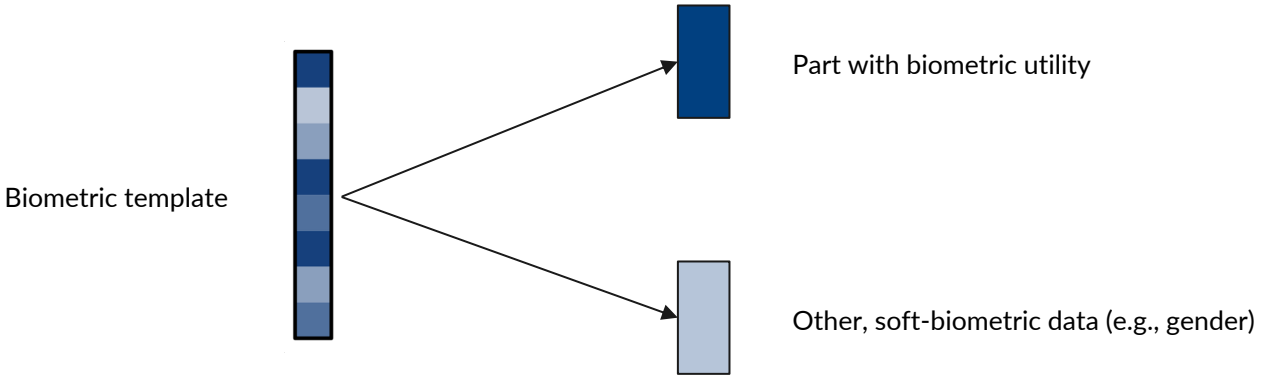
1. Image reconstruction from biometric face templates
2. Soft-biometric privacy-enhancing technologies
3. Workflow for irreversibility analysis
4. Experimental protocol, results
5. Future work

Introduction of the authors

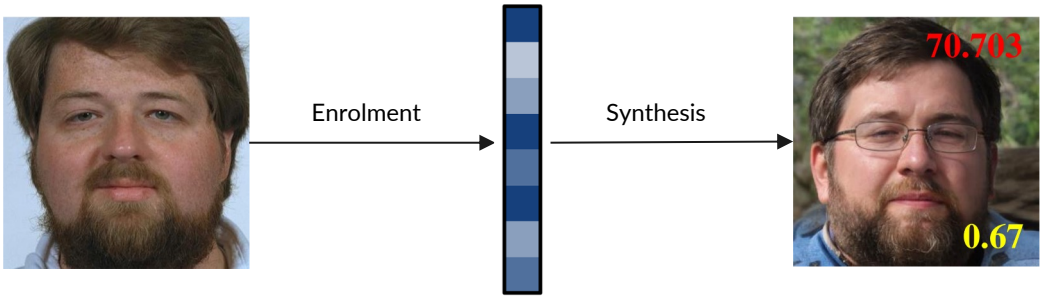
Dailé Osorio-Roig
Ph.D. student at Hochschule Darmstadt

Paul-Anton Gerlitz
Master student (Computer Science)
at Hochschule Darmstadt

Biometric templates



Reconstruction of biometric templates



Original sample | Biometric template | Reconstruction

Image source: Dong, X., Miao, Z., Ma, L., Shen, J., Jin, Z., Guo, Z., & Teoh, A. B. J. (2022). Reconstruct Face from Features Using GAN Generator as a Distribution Constraint (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2206.04295

Issues with soft-biometric data in biometric templates

Regulatory issue

Violates EU GDPR data minimization principle

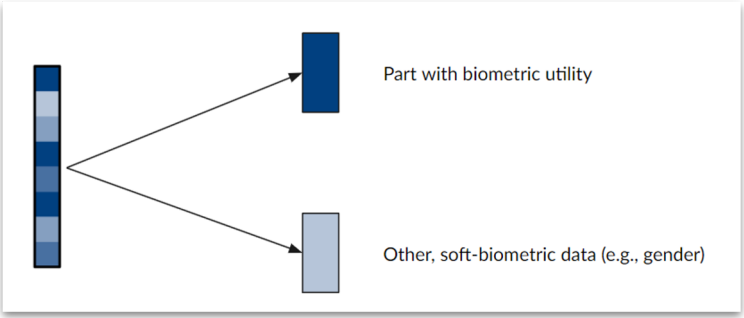
Security issue

Opens attack vector through impersonation

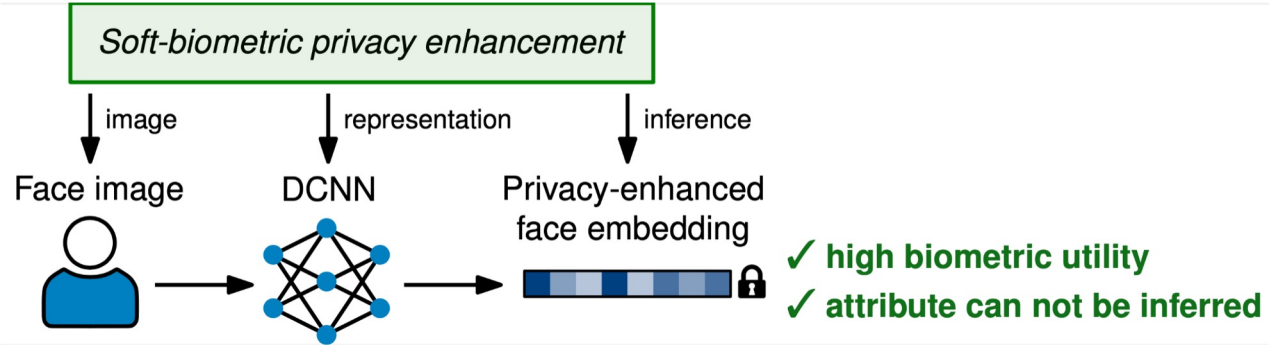
Privacy violation

Allows identification of subjects

Enables segmentation by attributes, e.g. gender



Soft-biometric Privacy-enhancing Technologies (PETs)



Enrolment using privacy-enhancement

Training-free privacy enhancement: PE-MIU

Proposed by P. Terhörst et al. (2020)

Permutates template randomly (Block shuffle)

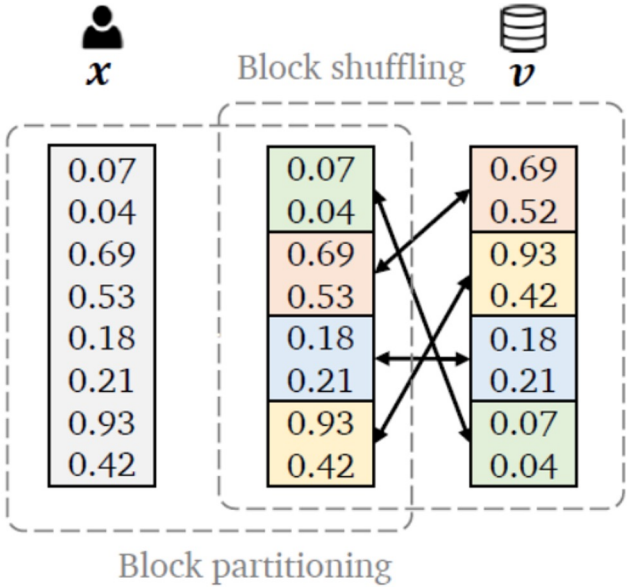


Image source: Terhorst, P., Riehl, K., Damer, N., Rot, P., Bortolato, B., Kirchbuchner, F., Struc, V., & Kuijper, A. (2020). PE-MIU: A Training-Free Privacy-Enhancing Face Recognition Approach Based on Minimum Information Units. In IEEE Access (Vol. 8, pp. 93635–93647). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/access.2020.2994960

PE-MIU: Security through probability (I)

PE-MIU block setting

Divides feature embedding into *N* blocks

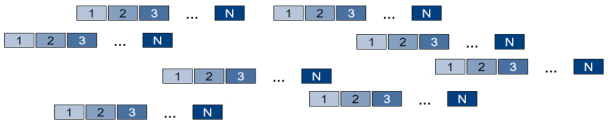
V divided into *N* number of blocks

PE-MIU random shuffle

Randomly permutate block order

N! possible permutations

Permutations have different level of complexity



V' has *N!* possible permutations

PE-MIU: Security through probability (II)

Permutation complexity

Number of blocks that have a different position in the shuffled vector

Example

Template (size 512) divided into
4 blocks (size 128)

$4!$

24 possible permutations

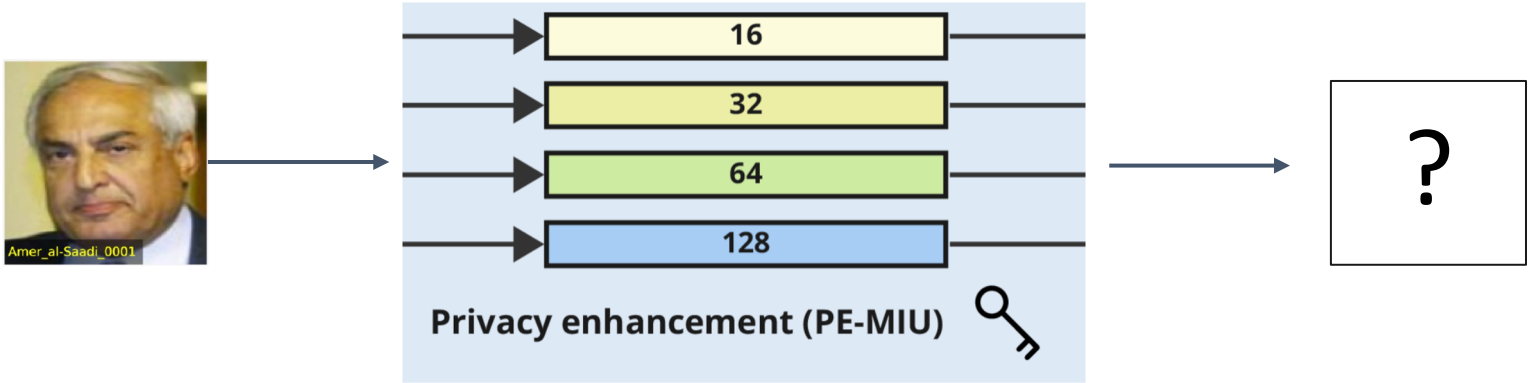
Permutation complexity 0:
No blocks changed position

Permutation complexity 3:
3 blocks changed position

Permutation complexity 2:
2 blocks changed position

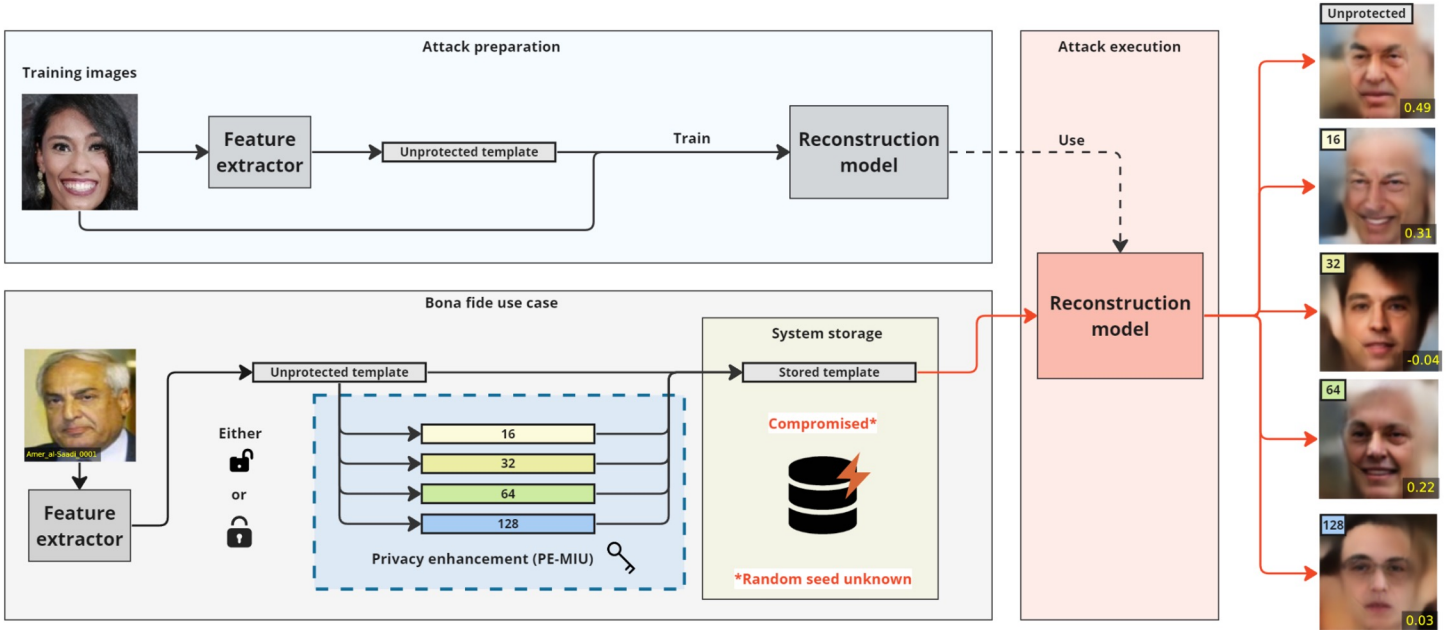
Permutation complexity 4:
4 blocks changed position
(“derangement”)

Analyzing the irreversibility of privacy-enhanced templates (I)



Is image reconstruction using privacy-enhanced templates possible?

Analyzing the irreversibility of privacy-enhanced templates (II)



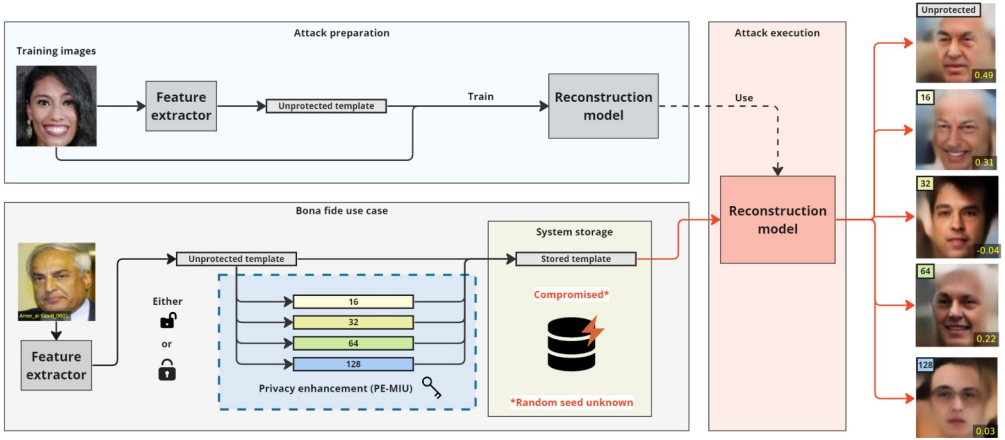
Training of inversion model; perform attack on unprotected and privacy-enhanced templates

Analyzing the irreversibility of privacy-enhanced templates (III)

Training on unprotected templates

Not specifically trained to adapt to

privacy-enhancement (PE-MIU)



Experimental protocol

Databases

Training: FFHQ

Evaluation: LFW

Feature extractors

ArcFace

Elasticface

PE-MIU settings

Different block size settings

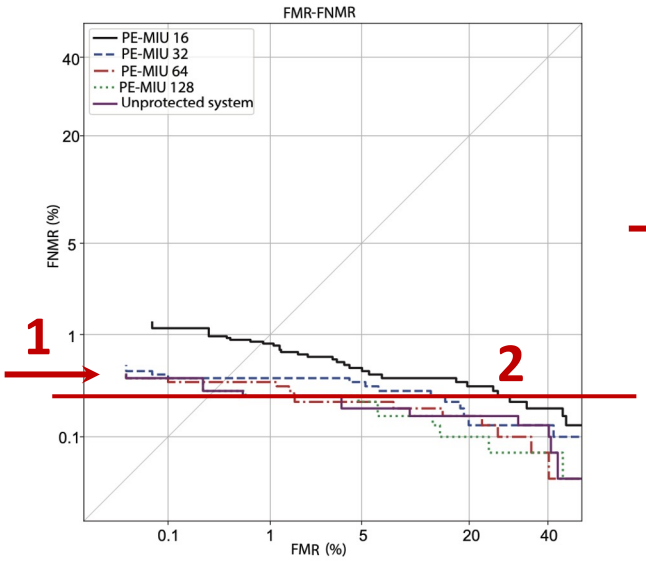
(16, 32, 64, 128)

Metrics for irreversibility evaluation

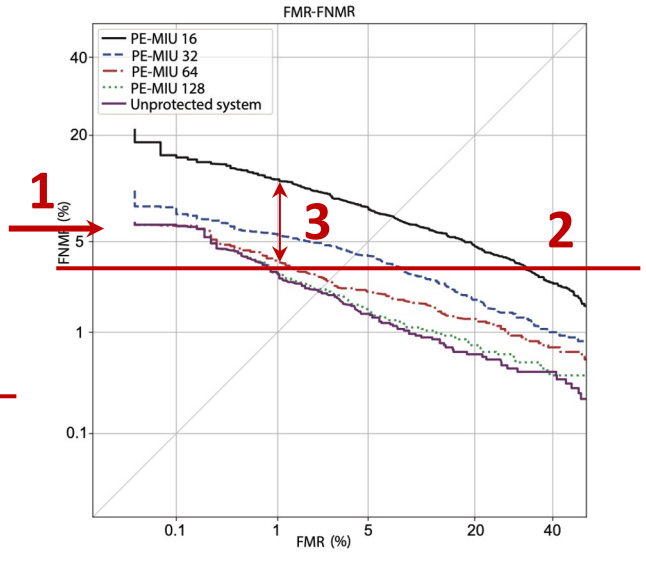
DET curves (FNMR, FMR, EER)

Reversibility success rate (%)

Results: Biometric performance



(a) ArcFace



(b) ElasticFace

1. Unprotected system performs best
2. PE-MIU performs better with ArcFace
3. Performance degradation correlates with block size

Results: Image reconstruction

Model	Protection	EER	FMR=0.1		FMR=1.0	
			FNMR	RSR	FNMR	RSR
ArcFace	Unprotected	0.30	0.40	**100.00**	0.27	**100.00**
	16	0.87	1.13	0.11	0.83	2.12
	32	0.40	0.40	0.60	0.40	4.66
	64	0.37	0.37	4.62	0.37	14.48
	128	0.30	0.40	19.22	0.27	34.65
ElasticFace	Unprotected	2.17	6.33	**99.63**	2.93	**99.82**
	16	7.27	15.67	0.08	12.00	1.04
	32	4.10	7.53	0.59	5.50	3.80
	64	2.63	6.37	5.32	3.63	15.42
	128	2.27	6.33	23.94	3.00	39.48

Reversibility success rates (RSR) at .1% / 1% security thresholds for unprotected and privacy-enhanced templates at varying block sizes

1. Unprotected templates can be reconstructed with almost 100% success
2. Privacy-enhanced templates cannot be reconstructed at block size 16 and 32.
3. Higher block size yields more reversibility success.

Results: Gender prediction accuracy

Model	Protection	SVM		
		Poly	RBF	Sigmoid
ArcFace	Unprotected	**0.81** ± 0.02	**0.89** ± 0.01	**0.85** ± 0.02
	16	0.50 ± 0.03	0.50 ± 0.03	0.49 ± 0.02
	32	0.50 ± 0.03	0.50 ± 0.03	0.49 ± 0.02
	64	0.52 ± 0.02	0.53 ± 0.03	0.52 ± 0.03
	128	0.55 ± 0.02	0.57 ± 0.02	0.56 ± 0.01
ElasticFace	Unprotected	**0.85** ± 0.02	**0.88** ± 0.02	**0.84** ± **0.02**
	16	0.52 ± 0.02	0.52 ± 0.03	0.51 ± 0.03
	32	0.52 ± 0.02	0.55 ± 0.02	0.54 ± 0.03
	64	0.57 ± 0.01	0.58 ± 0.03	0.57 ± 0.03
	128	0.64 ± 0.03	0.64 ± 0.02	0.63 ± 0.03

Gender prediction accuracy
for unprotected and privacy-enhanced templates at varying block sizes

1. Machine learning techniques are able to accurately predict the gender of unprotected templates with an accuracy of up to 89%
2. Gender of privacy-enhanced templates using PE-MIU cannot accurately be predicted

Image reconstruction w.r.t. permutation complexity of PE-MIU

Reversibility success rate at different fixed random seeds

Template (size 512) divided into 8 blocks (size 64)

8!

40,320 possible permutations

Permutations have different chances of occurring

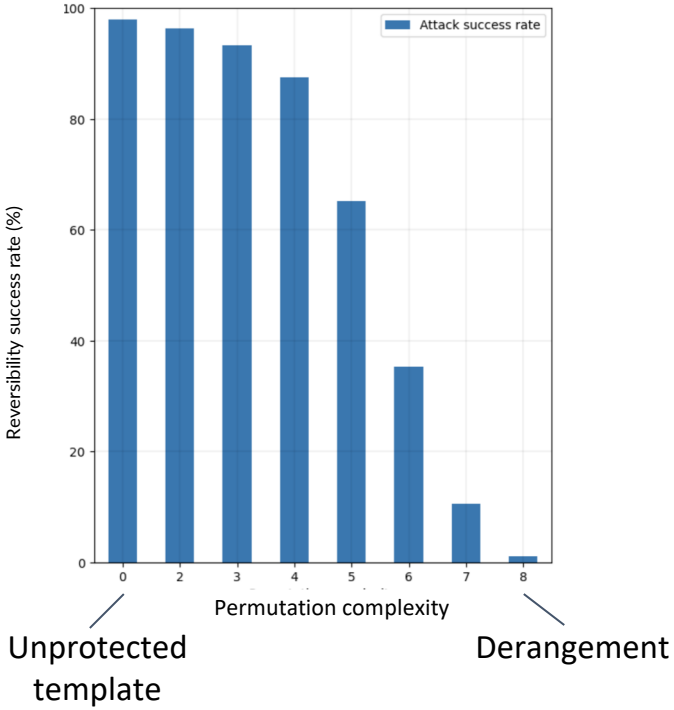
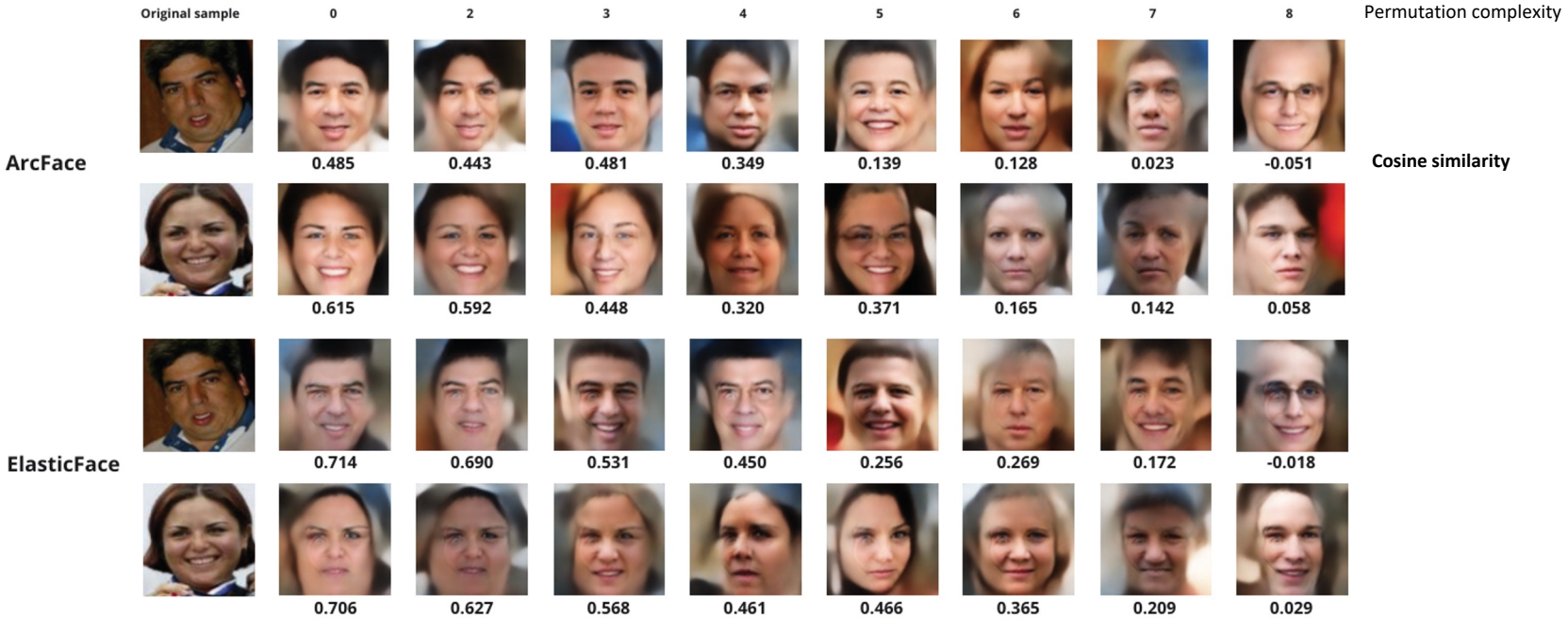


Image reconstruction w.r.t. permutation complexity of PE-MIU



Visual result of image reconstructions at varying permutation complexities

Results: Image reconstruction at different permutation complexities

Block size (K)	P	ArcFace		ElasticFace	
		FMR=0.1%	FMR=1.0%	FMR=0.1%	FMR=1.0%
32	4	89.09	96.64	97.83	99.86
	5	84.06	95.45	96.67	99.66
	6	78.59	93.51	92.39	99.15
	7	70.85	90.59	87.09	98.37
	8	58.44	85.39	75.77	95.65
	9	43.56	76.18	59.97	89.26
	10	32.79	67.01	44.10	79.95
	11	20.42	52.97	25.04	63.81
	12	9.68	36.29	10.26	43.39
	13	3.67	20.93	3.26	22.26
	14	1.39	9.85	0.85	7.37
	15	0.44	4.35	0.17	2.48
	16	0.0	1.39	0.00	0.48
64	2	88.96	96.33	98.03	99.69
	3	78.49	93.24	92.05	99.15
	4	60.45	87.53	75.33	95.17
	5	30.82	65.14	40.27	78.63
	6	9.58	35.37	9.0	38.63
	7	1.22	10.50	0.78	9.04
	8	0.07	1.16	0.00	0.37
128	2	60.58	85.93	75.94	95.62
	3	8.83	32.76	8.97	40.13
	4	0.03	1.19	0.00	0.37

1. Samples were shuffled using PE-MIU with a fixed random seed
2. With block size 64 and half of the blocks shuffled (permutation complexity 4), reconstruction success is at 87% (95%) for ArcFace (ElasticFace)
3. High permutation complexity makes reconstruction unsuccessful

Future work

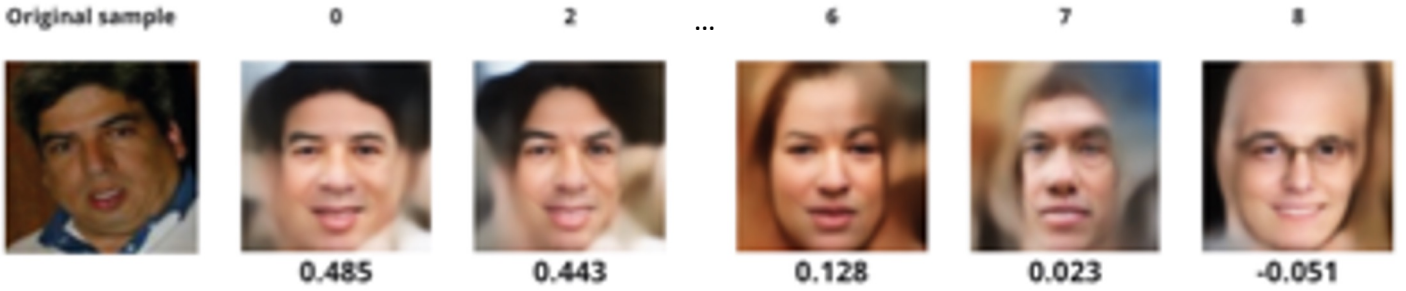
Attack PE-MIU reconstruction method

- PE-MIU uses a second sample from the same subject to undo the random shuffle
- Are there other ways or patterns to determine the original block order?

Increase attack success by limiting on samples with low permutation complexity

- Knowing the permutation complexity of a sample
- Limit attacks to samples that are susceptible

Conclusion



PE-MIU provides good security against image reconstruction and gender prediction attacks

Security is based on probability

Due to the random nature of the block shuffle, some protected templates are almost unchanged

Reversing Deep Face Embeddings with Probable Privacy Protection

Dailé Osorio-Roig, Paul A. Gerlitz, Christian Rathgeb, and Christoph Busch

da/sec – Biometrics and Security Research Group
Hochschule Darmstadt

Thank you for your attention.
Questions?

https://www.linkedin.com/in/paulantongerlitz/