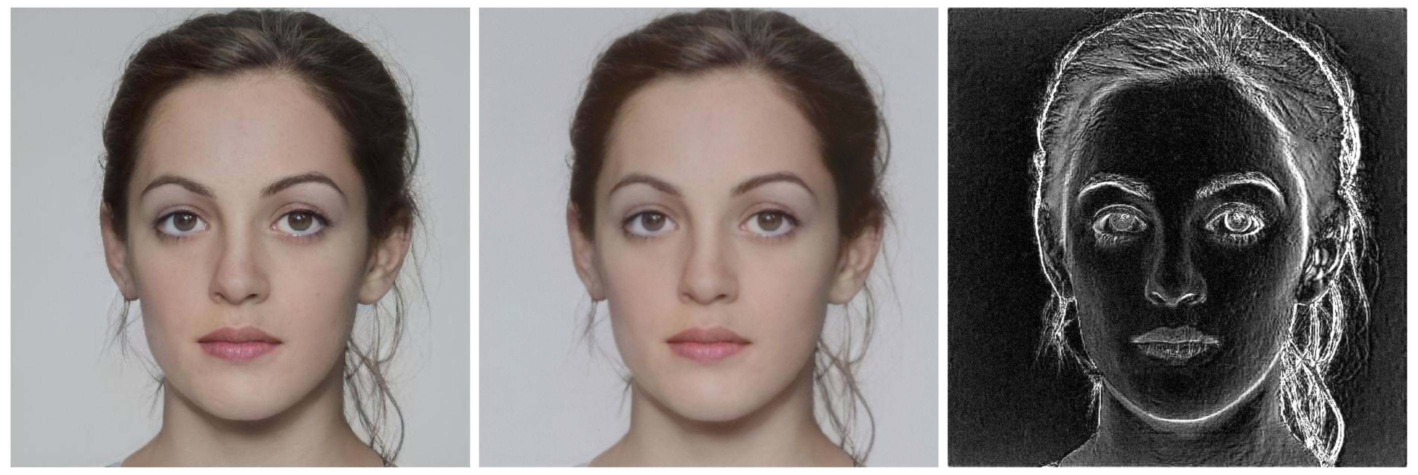
The Impact of Print-and-Scan in Heterogeneous Morph Evaluation Scenarios

Richard E. Neddo   Zander W. Blasingame   Chen Liu

Department of Electrical and Computer Engineering
Clarkson University
{neddore, blasinzw, cliu}@clarkson.edu

IEEE International Joint Conference on Biometrics

Motivation



(a) Digitally Morphed Image (b) Print-Scanned Morphed image (c) Amplified Print-scan Artifacts

Figure 1. Example of a morph before and after undergoing print-scanning. Samples are from the FRLL dataset [1].

- **Print-scanned** Diffusion Morphs (DiM) which are a recent SOTA algorithm for creating face morphs [2]
- Introducing print-scanned elements into an evaluation with digital images creates uncertainty in Single-image Morphing Attack Detection (S-MAD).
- Print-Scanned and digital morphs currently are not evaluated against print-scanned bona fides.
- We propose a heterogeneous attack configuration where during evaluation a detector should be trained to detect images that contain elements that are both digital and print-scanned in nature.

Table 1. Attack scenarios to evaluate impact of heterogeneous data

Configuration	Morph	Bona Fide
D-D	Digital	Digital
D-PS	Digital	Print-Scanned
PS-D	Print-Scanned	Digital
PS-PS	Print-Scanned	Print-Scanned

Methodology

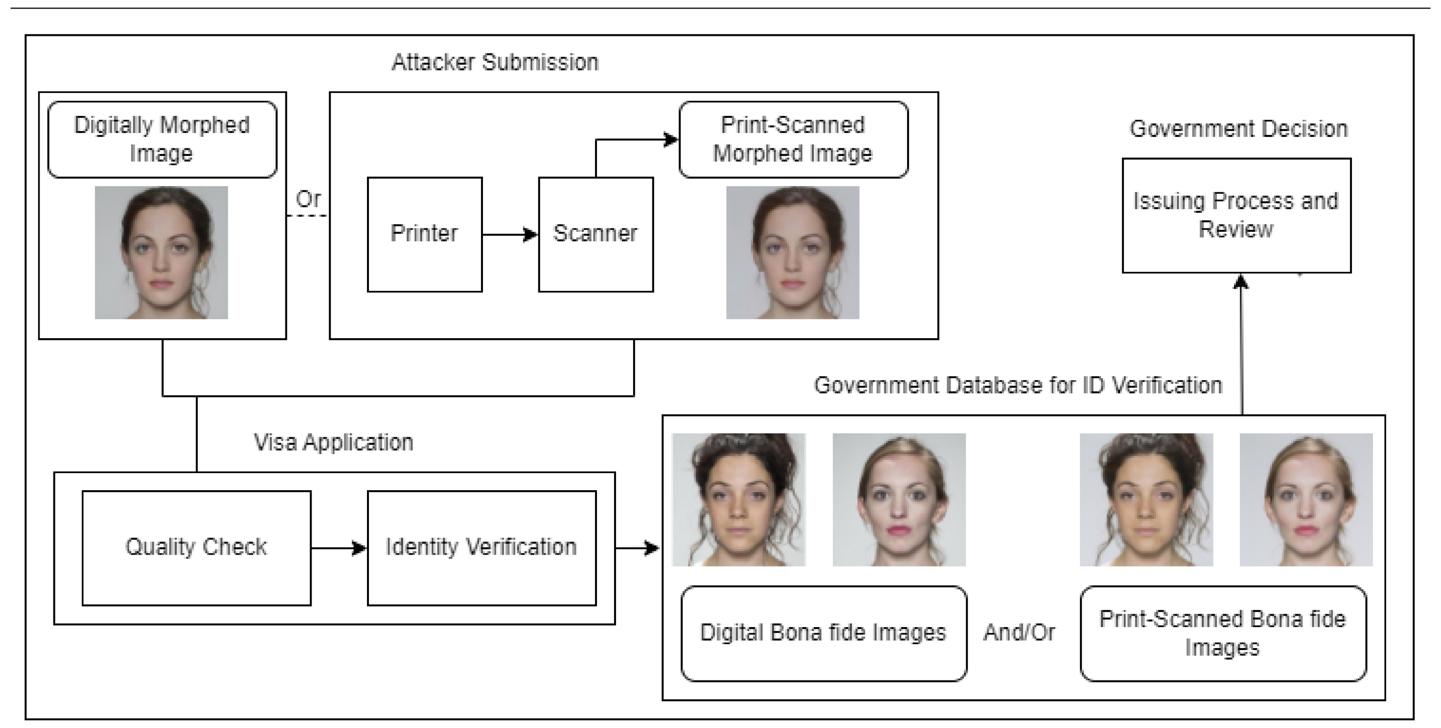
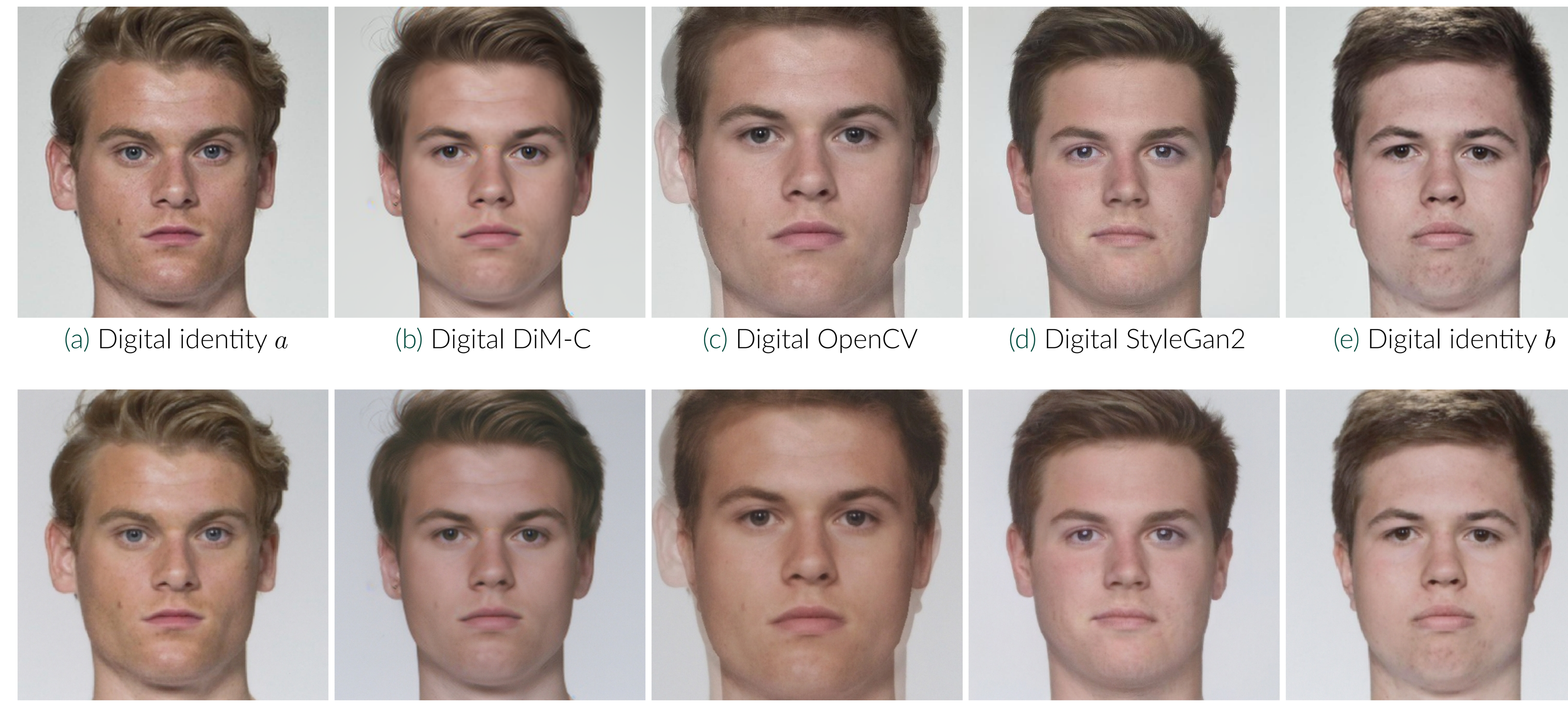


Figure 2. Heterogeneous morph attack pipeline in a simulated real-world scenario.

- Images are digitally arranged on an 8.5×12 inch blank PNG. JavaScript scripts are used to send the pages to Adobe Photoshop for print management to maintain ICC profiles.
- A Canon Pixma Pro 100 Printer and Epson 850v Pro Scanner were used for printing and scanning. All print-scanned images were set at a 600×600 resolution with a pixel-per-inch value of 300 to replicate a passport photo of size two inches by 2 inches while also maintaining their original aspect ratio.
- Images are saved as Portable Network Graphics (PNG) files without compression to avoid adding additional artifacts.
- The morphs, component identity pairs, and alternate bona fide identity images were print-scanned for evaluation. This resulted in 8,142 morphs and 4,653 bona fide images being print-scanned. This work used the bona fide pairs developed in [3] for our FRGC, FERET, and FRLL pairings and was used to create the DiM, OpenCV, and StyleGAN2 morphs.

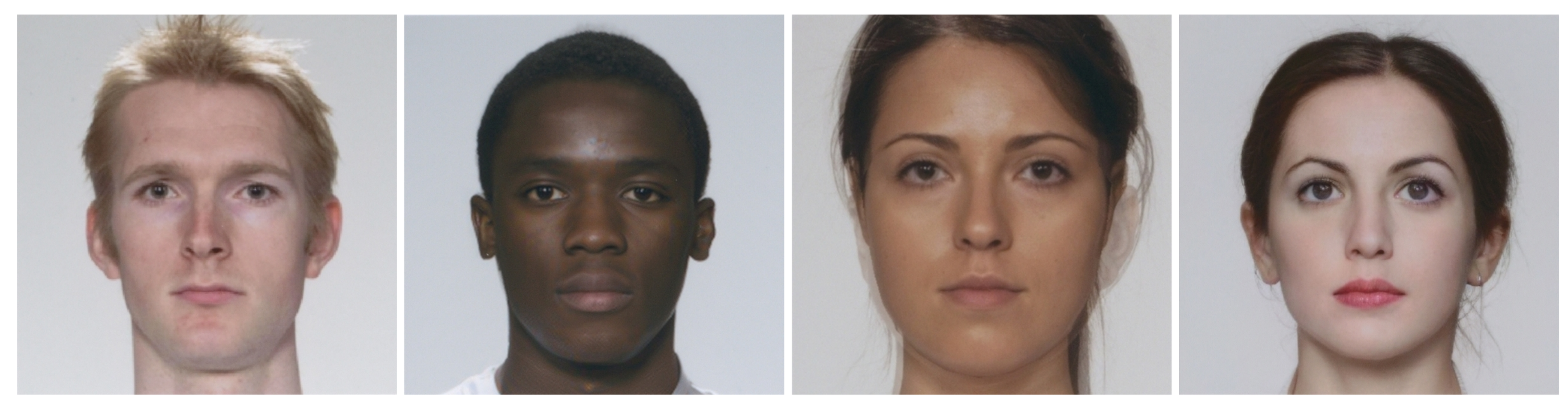
Vulnerablity Study



(a) Digital identity a (b) Digital DiM-C (c) Digital OpenCV (d) Digital StyleGan2 (e) Digital identity b

(f) PS identity a (g) PS DiM-C (h) PS OpenCV (i) PS StyleGan2 (j) PS identity b

Figure 3. Comparison of morphs on the FRLL dataset.



(a) PS bona fide (b) PS DiM-C (c) PS OpenCV (d) PS StyleGan2

Figure 4. Additional print-scanned morphs and bona fides

- Evaluated proposed attack scenario to compare digital and print-scanned images against each set of bona fides as seen in Table 1.
- Evaluated on the OpenCV [3], StyleGAN2 [3], and DiM [2] morphing attacks.
- Used three FR systems representing the SOTA: ArcFace [4], AdaFace [5], and ElasticFace [6].
- The ProdAvg Mated Morph Presentation Match Rate (MMPMR) metric [7] is defined as

$$M(\delta) = \frac{1}{M}\sum_{m=1}^{M}\left[\prod_{n=1}^{N_m}\left(\frac{1}{I_m^n}\sum_{i=1}^{I_m^n}\{S_m^{n,i} > \delta\}\right)\right] \quad (1)$$

where δ is the verification threshold, S_m^n is the similarity score of the n-th subject of morph m, N_m is the total number of contributing subjects to morph m, M is the total number of morphed images, and I_m^n is the number of samples of the subject n compared to morph m.

Table 2. MMPMR for all scenarios with FMR = 0.1%. A higher MMPMR value represents a stronger attack.

		FRLL			FRGC			FERET		
Morph	Scenario	ArcFace	ElasticFace	AdaFace	ArcFace	ElasticFace	AdaFace	ArcFace	ElasticFace	AdaFace
OpenCV	D-D	99.02	**98.69**	**99.26**	67.31	**50.99**	53.22	89.04	75.61	81.78
	D-PS	**99.18**	97.22	99.02	68.91	47.81	53.96	**89.97**	**81.66**	**83.51**
	PS-D	98.61	96.81	97.87	55.67	43.15	45.36	86.45	78.48	81.95
	PS-PS	98.85	94.19	99.02	**69.89**	41.61	**55.51**	88.82	78.58	77.13
StyleGAN2	D-D	5.89	3.27	6.55	**1.38**	1.21	1.25	0.82	0.32	0.72
	D-PS	3.44	**5.56**	4.66	0.67	**1.28**	**1.45**	**0.82**	**0.41**	**1.29**
	PS-D	5.32	1.31	**7.53**	1.00	1.00	0.56	0	0	0
	PS-PS	**6.63**	3.11	6.38	0.41	0.44	1.36	0	0	0
DiM-C	D-D	92.88	82.00	88.22	48.70	**43.24**	41.75	69.76	59.65	65.27
	D-PS	90.10	**88.95**	87.81	43.65	39.23	42.66	71.53	62.39	68.46
	PS-D	92.39	77.09	**91.33**	**49.11**	37.98	35.82	**74.03**	62.21	65.08
	PS-PS	**93.62**	83.22	90.83	37.47	28.30	**44.04**	66.91	**64.20**	**69.99**

- When looking at any DiM-C morph scenario containing a print-scanned element, the scenarios perform better 89% of the time at an average of 5.01% with a maximum difference of 8.48%.
- Similar performance can be observed across the OpenCV scenarios that contain a print-scanned element. 67% of the morph scenarios perform better than the D-D scenario as a baseline averaging 3.17% with a maximum difference of 8%.
- Proposed approach illustrates the impact of heterogeneous media types across all data where FRs are more vulnerable to attacks containing a print-scanned element.

Detection Study

Table 3. S-MAD Study with training by varying OpenCV Morphs with bona fides on FRGC.

		Digital				Digital + Print-Scan				Print-Scan			
			MACER @ BPCER				MACER @ BPCER				MACER @ BPCER		
Morphing Attack	Scenario	EER	0.1%	1.0%	5.0%	EER	0.1%	1.0%	5.0%	EER	0.1%	1.0%	5.0%
OpenCV	D-D	0	0	0	0	0	0	0	0	4.81	71.76	26.93	4.64
	PS-D	0.82	77.25	0.63	0.13	0	0	0	0	0	0	0	0
	D-PS	0	0	0	0	0	0	0	0	**11.78**	**88.55**	**61.32**	**26.66**
	PS-PS	**13.63**	**96.12**	**70.7**	**39.37**	0	0	0	0	0	0	0	0
StyleGAN2	D-D	0.13	0.13	0.07	0	0.1	0.1	0	0	9.97	97.33	78.41	30.74
	PS-D	6.65	96.51	47.56	10.14	0.23	0.49	0	0	0.43	7.04	0.03	0
	D-PS	1.91	68.6	5.96	0.56	0.86	7.83	0.79	0.1	**25.61**	**99.61**	**85.39**	**65.01**
	PS-PS	**31.47**	**99.74**	**97.5**	**79.66**	**2.57**	**48.85**	**6.65**	**1.09**	2.27	48.45	8.62	0.69
DiM-C	D-D	7.67	87.03	**55.63**	13.2	**15.14**	**99.8**	**91.67**	**52.21**	**39.43**	99.57	96.61	87.2
	PS-D	7.9	**92.43**	44.67	14.35	1.55	46.18	2.24	0.43	2.7	67.18	5.76	0.72
	D-PS	0.3	4.34	0	0	1.25	20.67	1.58	0.26	36.87	**100**	**99.61**	**92.13**
	PS-PS	**9.97**	87.52	50.2	**23.5**	2.9	68.89	7.27	1.15	7.27	91.47	51.58	13.43

Table 4. S-MAD Study with training by varying DiM-C Morphs with bona fides on FRGC.

		Digital				Digital + Print-Scan				Print-Scan			
			MACER @ BPCER				MACER @ BPCER				MACER @ BPCER		
Morphing Attack	Scenario	EER	0.1%	1.0%	5.0%	EER	0.1%	1.0%	5.0%	EER	0.1%	1.0%	5.0%
OpenCV	D-D	4.08	70.9	13.03	3.39	3.59	49.7	14.94	2.47	13.69	92.2	67.94	29.13
	PS-D	25.18	97.63	87.56	65.54	0.3	1.55	0.2	0.07	0.03	0.03	0.03	0
	D-PS	1.78	39.53	2.83	0.53	5.69	82.55	39.8	6.81	**17.12**	**96.84**	**80.09**	**41.31**
	PS-PS	**41.51**	**98.49**	**93.42**	**85.94**	**15.8**	**92.36**	**83.11**	**47.7**	8.29	94.31	50.63	13.66
StyleGAN2	D-D	8.72	97.2	46.38	16.66	2.17	80.94	5.92	0.36	6.22	84.69	51.48	7.27
	PS-D	17.38	98.49	84.13	57.93	0.36	0.56	0.26	0.07	0.3	0.63	0.03	0
	D-PS	10.53	91.08	60.5	27.52	7.67	**98.12**	52.01	14.02	**18.27**	**99.93**	**88.78**	**57.04**
	PS-PS	**33.18**	**99.77**	**95.06**	**81.34**	**11.09**	94.6	**81.5**	**30.22**	6.75	91.71	32.13	8.69
DiM-C	D-D	0	0	0	0	**0.07**	**0.07**	0	0	**11.52**	**99.08**	**87.66**	**33.67**
	PS-D	2.07	**69.95**	**10.43**	0.33	0	0	0	0	0	0	0	0
	D-PS	0	0	0	0	0	0	0	0	1.91	38.71	4.11	0.95
	PS-PS	**2.5**	65.67	8.13	**0.92**	0.03	0.03	0	0	0.1	0.39	0	0

- *Morphing Attack Classification Error Rate* at a *Bona Fide Presentation Classification Error Rate* (MACER @ BPCER) metric is defined to quantify the rate at which morphing attacks are incorrectly classified as genuine biometric samples (MACER) while maintaining a specified rate at which genuine biometric samples are incorrectly classified as fraudulent (BPCER)s.
- S-MAD performance relies heavily on input training data. When trained on DiM-C morphs the OpenCV morphs had decreased detection rates. This trend is also seen with the Print-Scan trained S-MAD not detecting digital morphs.
- The low rates of detection observed with data not associated with the input training data demonstrate venerability when detecting heterogeneous morphed images.

Conclusion

- Developed print-scanned morph and bona fides that nominally outperform digital counterparts.
- Trained S-MAD to detect digitally morphed images and print-scanned morphed images.
- Developed a novel strategy to incorporate mixed media types into evaluation scenarios.
- Demonstrated the importance of input data for training detectors.
- Evaluation scenarios can be expanded to incorporate simulated print-scanned data and more types of morphs.

References

[1] L. DeBruine and B. Jones, "Face Research Lab London Set," 5 2017.

[2] Z. W. Blasingame and C. Liu, "Leveraging diffusion for strong and high quality face morphing attacks," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 6, no. 1, pp. 118–131, 2024.

[3] E. Sarkar, P. Korshunov, L. Colbois, and S. Marcel, "Are gan-based morphs threatening face recognition?," in *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2959–2963, 2022.

[4] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4690–4699, 2019.

[5] M. Kim, A. K. Jain, and X. Liu, "Adaface: Quality adaptive margin for face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022.

[6] F. Boutros, N. Damer, F. Kirchbuchner, and A. Kuijper, "Elasticface: Elastic margin loss for deep face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pp. 1578–1587, June 2022.

[7] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. J. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Ramachandra, and C. Busch, "Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting," in *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp. 1–7, 2017.

Supported by CITeR and NSF under Grant # 1650503