PRO-Face: A Generic Framework for Privacy-preserving Recognizable Obfuscation of Face Images

Supplementary materials

ACM Reference Format:
Supplementary materials. 2022. PRO-Face: A Generic Framework for Privacy-preserving Recognizable Obfuscation of Face Images. In *Proceedings of the 30th ACM International Conference on Multimedia (MM '22), October 10–14, 2022, Lisboa, Portugal.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3503161.3548202

A MORE DETAILS ON EXPERIMENT SETUPS

A.1 Face recognizers

The recognition models used in our experiments are obtained from publicly available GitHub repositories:

- https://github.com/timesler/facenet-pytorch for Inception-ResNet [8].
- https://github.com/deepinsight/insightface/tree/master/recognition/arcface_torch for MobileFaceNet [3], IResNet50 [4] and IResNet100 [4].
- https://github.com/QuasarLight/Pytorch_Face_Recognition for the SEResNet50 [5].

All selected models achieve satisfactory recognition performance on LFW (shown in the main manuscript). We opt for using publicly available pre-trained models instead of training them by ourself for two considerations:

(1) Those models are trained on another dataset (CISIA-Webface [9]) different from the ones used in our evaluation. This further increases the generalization of the proposed framework, given the fact that training of our protection model is irrelevant to the training of the recognizers.
(2) This setup also coincides with the realistic scenarios where PRO-Face may be used: An organization (such as university) already possesses a face recognizer either provided by a third-party or trained by themselves, on any face dataset. The organization needs to protect the privacy of individuals captured by their recognition systems. Therefore, it can easily train such a PRO-Face protection model on any other dataset it has access to without retraining the recognizer.

A.2 More details of user study on MTurk

Figure 1 and 2 illustrate a normal test question for subjective privacy evaluation and a "honypot" question respectively.

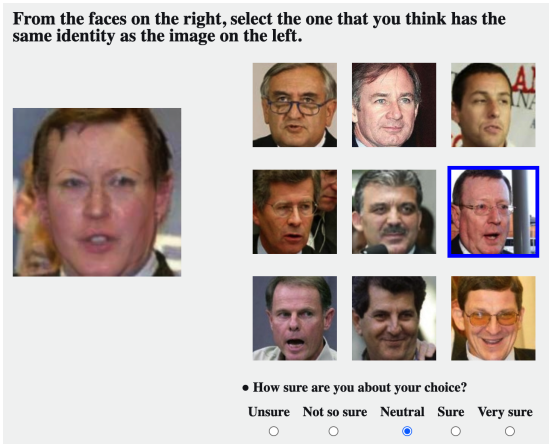

Figure 1: A test image under evaluation on MTurk. We reward each subject 0.02 US Dollars for completing each HIT.

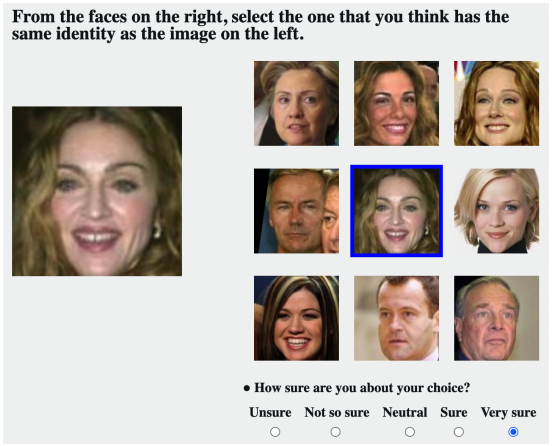

Figure 2: A "honypot" question on Mturk where the test image that also appears in the candidate list, which should be very easy for subjects to identity. This is to eliminate sloppy subjects who give random answers.

B ADDITIONAL EVALUATION RESULTS

To supplement the main manuscript, we show addition evaluation results of privacy protection and utility preservation on CelebA [7] and VGGFace2 [1]. Table 1 and 2 show the privacy scores measured by similarity metrics on CelebA and VGGFace2 respectively. Table 3 and 4 show the verification performance of different recognizers on PRO-Face protected images on CelebA and VGGFace2 respectively.

MM '22, October 10–14, 2022, Lisboa, Portugal

ACM ISBN 978-1-4503-9203-7/22/10…$15.00
https://doi.org/10.1145/3503161.3548202

Obfuscation ▷	Blur		Pixelate		FaceShifter [6]		SimSwap [2]	
Recognizer ▽	LPIPS ↑	SSIM ↓	LPIPS ↑	SSIM ↓	LPIPS ↑	SSIM ↓	LPIPS ↑	SSIM ↓
MobileFaceNet [3]	0.470	0.586	0.638	0.513	0.108	0.851	0.175	0.774
InceptionResNet [8]	0.460	0.618	0.635	0.560	0.099	0.867	0.166	0.791
IResNet50 [4]	0.463	0.604	0.638	0.541	0.102	0.866	0.171	0.781
SEResNet50 [5]	0.473	0.588	0.639	0.517	0.102	0.866	0.172	0.775
IResNet100 [4]	0.454	0.600	0.634	0.555	0.103	0.855	0.168	0.787

Table 1: Objective measurement of privacy by similarity between protected and original images on CelebA [7].

Obfuscation ▷	Blur		Pixelate		FaceShifter [6]		SimSwap [2]	
Recognizer ▽	LPIPS ↑	SSIM ↓	LPIPS ↑	SSIM ↓	LPIPS ↑	SSIM ↓	LPIPS ↑	SSIM ↓
MobileFaceNet	0.454	0.597	0.638	0.527	0.126	0.831	0.185	0.804
InceptionResNet	0.439	0.633	0.634	0.575	0.115	0.849	0.174	0.822
IResNet50	0.448	0.617	0.638	0.556	0.120	0.848	0.181	0.811
SEResNet50	0.459	0.599	0.639	0.531	0.120	0.847	0.181	0.805
IResNet100	0.439	0.612	0.634	0.573	0.117	0.840	0.174	0.822

Table 2: Objective measurement of privacy by similarity between protected and original images on VGGFace2 [1].

Obfuscation ▷	Blur		Pixelate		FaceShifter		SimSwap	
Recognizer ▽	ADR	XDR	ADR	XDR	ADR	XDR	ADR	XDR
MobileFaceNet	0.754/0.916	0.806/0.923	0.744/0.921	0.769/0.919	0.844/0.937	0.681/0.870	0.868/0.947	0.706/0.879
InceptionResNet	0.763/0.939	0.860/0.956	0.702/0.921	0.809/0.944	0.876/0.957	0.866/0.955	0.898/0.960	0.882/0.957
IResNet50	0.771/0.931	0.840/0.940	0.768/0.922	0.800/0.927	0.891/0.958	0.814/0.926	0.895/0.962	0.782/0.926
SEResNet50	0.737/0.915	0.820/0.932	0.705/0.905	0.758/0.916	0.880/0.957	0.834/0.929	0.891/0.960	0.795/0.920
IResNet100	0.866/0.942	0.931/0.950	0.701/0.909	0.857/0.930	0.941/0.973	0.906/0.946	0.937/0.978	0.894/0.946

Table 3: Face verification performance of PRO-Face in terms of TAR w.r.t. different obfuscations and recognizers on CelebA [7]. Two values split by / indicate TAR @ FAR = 0.01 and 0.1 respectively. ADR/XDR indicate Anonymous-/Cross-domain respectively.

Obfuscation ▷	Blur		Pixelate		FaceShifter		SimSwap	
Recognizer ▽	ADR	XDR	ADR	XDR	ADR	XDR	ADR	XDR
MobileFaceNet	0.406/0.842	0.559/0.842	0.530/0.846	0.610/0.864	0.622/0.830	0.441/0.803	0.644/0.842	0.514/0.805
InceptionResNet	0.613/0.895	0.713/0.911	0.435/0.832	0.581/0.890	0.769/0.926	0.756/0.921	0.764/0.939	0.762/0.935
IResNet50	0.572/0.842	0.629/0.871	0.583/0.847	0.644/0.858	0.647/0.900	0.539/0.861	0.612/0.866	0.528/0.840
SEResNet50	0.468/0.854	0.589/0.863	0.475/0.781	0.562/0.827	0.677/0.874	0.576/0.863	0.648/0.874	0.537/0.829
IResNet100	0.734/0.902	0.842/0.915	0.620/0.844	0.732/0.874	0.823/0.909	0.828/0.892	0.783/0.898	0.786/0.876

Table 4: Face verification performance of PRO-Face in terms of TAR w.r.t. different obfuscations and recognizers on VGGFace2 [1]. Two values split by / indicate TAR @ FAR = 0.01 and 0.1 respectively. ADR/XDR indicate Anonymous-/Cross-domain respectively.

C ADDITIONAL EXAMPLE IMAGES

Furthermore, additional example images protected by PRO-Face with respect to different obfuscations and face recognizers are given in Figures 3 to 7.

REFERENCES

[1] Qiong Cao, Li Shen, Weidi Xie, Omkar M. Parkhi, and Andrew Zisserman. 2018. VGGFace2: A Dataset for Recognising Faces across Pose and Age. In *2018 13th IEEE International Conference on Automatic Face Gesture Recognition (FG 2018)*. 67–74.

[2] Renwang Chen, Xuanhong Chen, Bingbing Ni, and Yanhao Ge. 2020. SimSwap: An Efficient Framework For High Fidelity Face Swapping. In *Proceedings of the 28th ACM International Conference on Multimedia (MM 2020)*. 2003–2011.

[3] Sheng Chen, Yang Liu, Xiang Gao, and Zhen Han. 2018. MobileFaceNets: Efficient CNNs for Accurate Real-Time Face Verification on Mobile Devices. In *Chinese Conference on Biometric Recognition (CCBR 2018)*. 428–438.

[4] Ionut Cosmin Duta, Li Liu, Fan Zhu, and Ling Shao. 2021. Improved Residual Networks for Image and Video Recognition. In *2020 25th International Conference on Pattern Recognition (ICPR 2020)*. 9415–9422.

[5] Jie Hu, Li Shen, Samuel Albanie, Gang Sun, and Enhua Wu. 2020. Squeeze-and-Excitation Networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI)* 42, 8 (2020), 2011–2023.

[6] Lingzhi Li, Jianmin Bao, Hao Yang, Dong Chen, and Fang Wen. 2020. Advancing High Fidelity Identity Swapping for Forgery Detection. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2020)*. 5073–5082.

[7] Ziwei Liu, Ping Luo, Xiaogang Wang, and Xiaoou Tang. 2015. Deep Learning Face Attributes in the Wild. In *2015 IEEE International Conference on Computer Vision (ICCV 2015)*. 3730–3738.

[8] Christian Szegedy, Sergey Ioffe, Vincent Vanhoucke, and Alexander A. Alemi. 2017. Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. In *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (AAAI 2018)*. 4278–4284.

[9] Dong Yi, Zhen Lei, Shengcai Liao, and Stan Z. Li. 2014. Learning Face Representation from Scratch. https://arxiv.org/abs/1411.7923

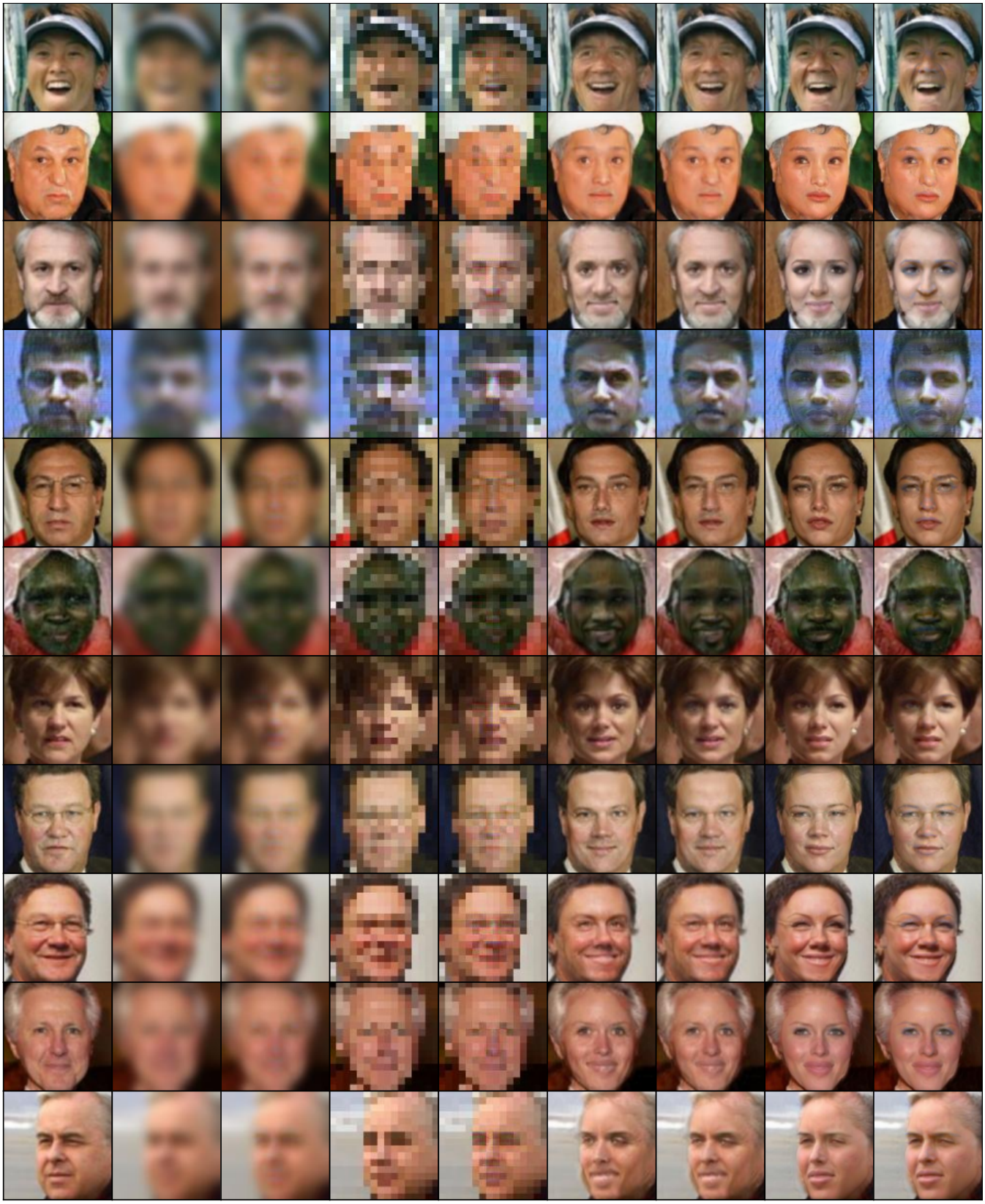

Figure 3: Example images in different protected forms with respect to the face recognizer MobileFaceNet. The symbol ⋆ indicates PRO-Face protected image corresponding to the obfuscation.

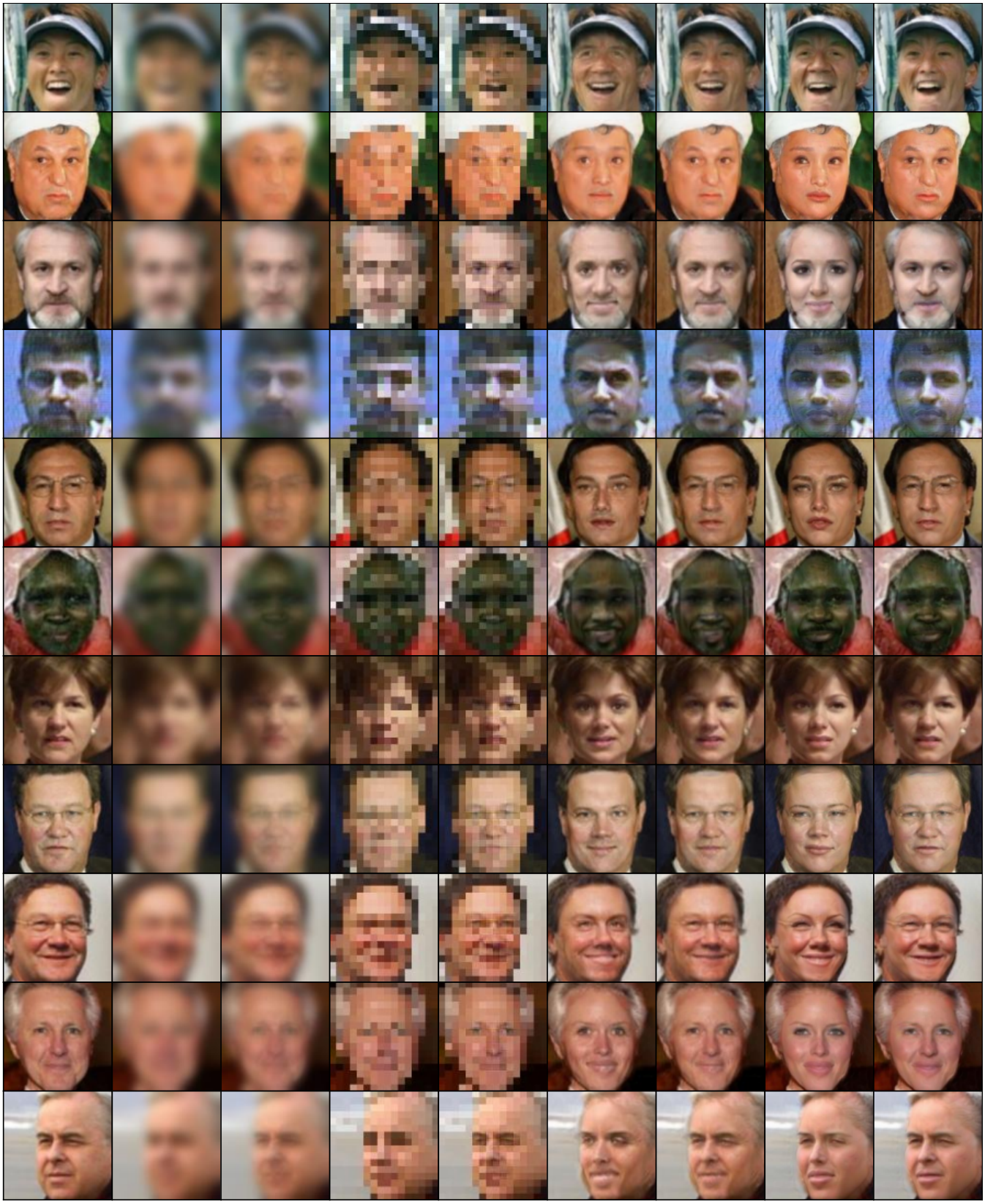

Figure 4: Example images in different protected forms with respect to the face recognizer InceptionResNet. The symbol ⋆ indicates PRO-Face protected image corresponding to the obfuscation.

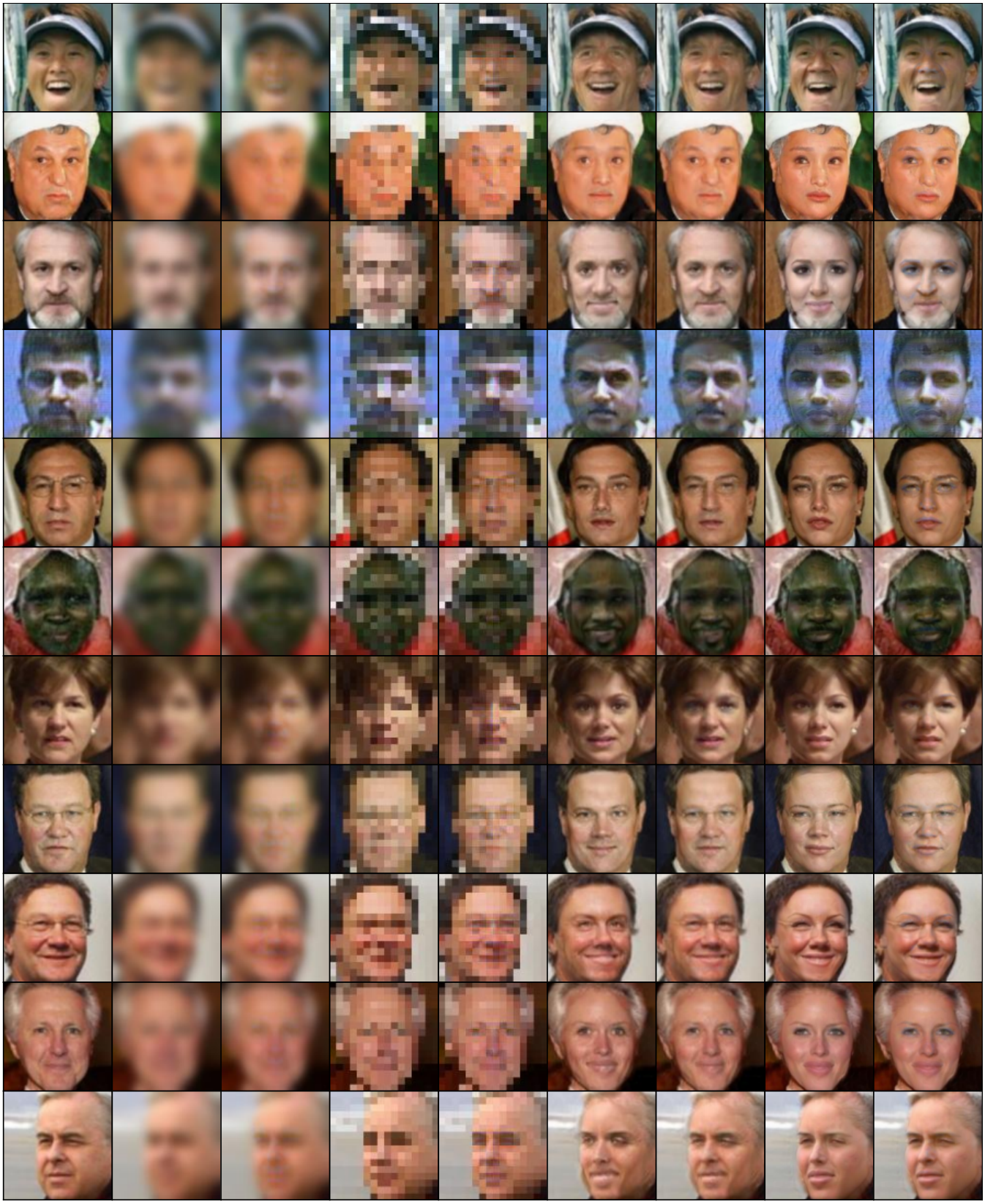

Figure 5: Example images in different protected forms with respect to the face recognizer IResNet50. The symbol ⋆ indicates PRO-Face protected image corresponding to the obfuscation.

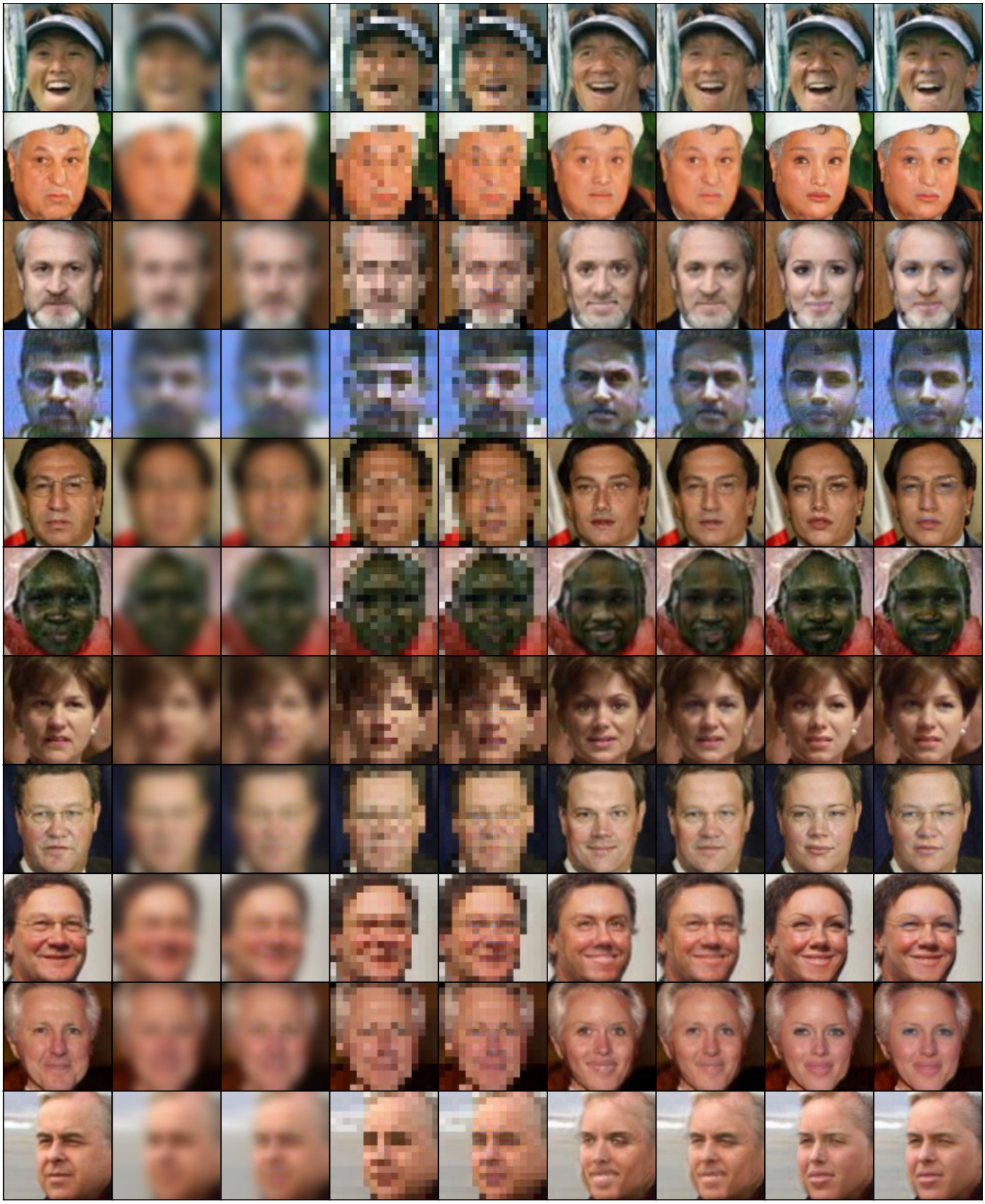

Figure 6: Example images in different protected forms with respect to the face recognizer SEResNet50. The symbol ⋆ indicates PRO-Face protected image corresponding to the obfuscation.

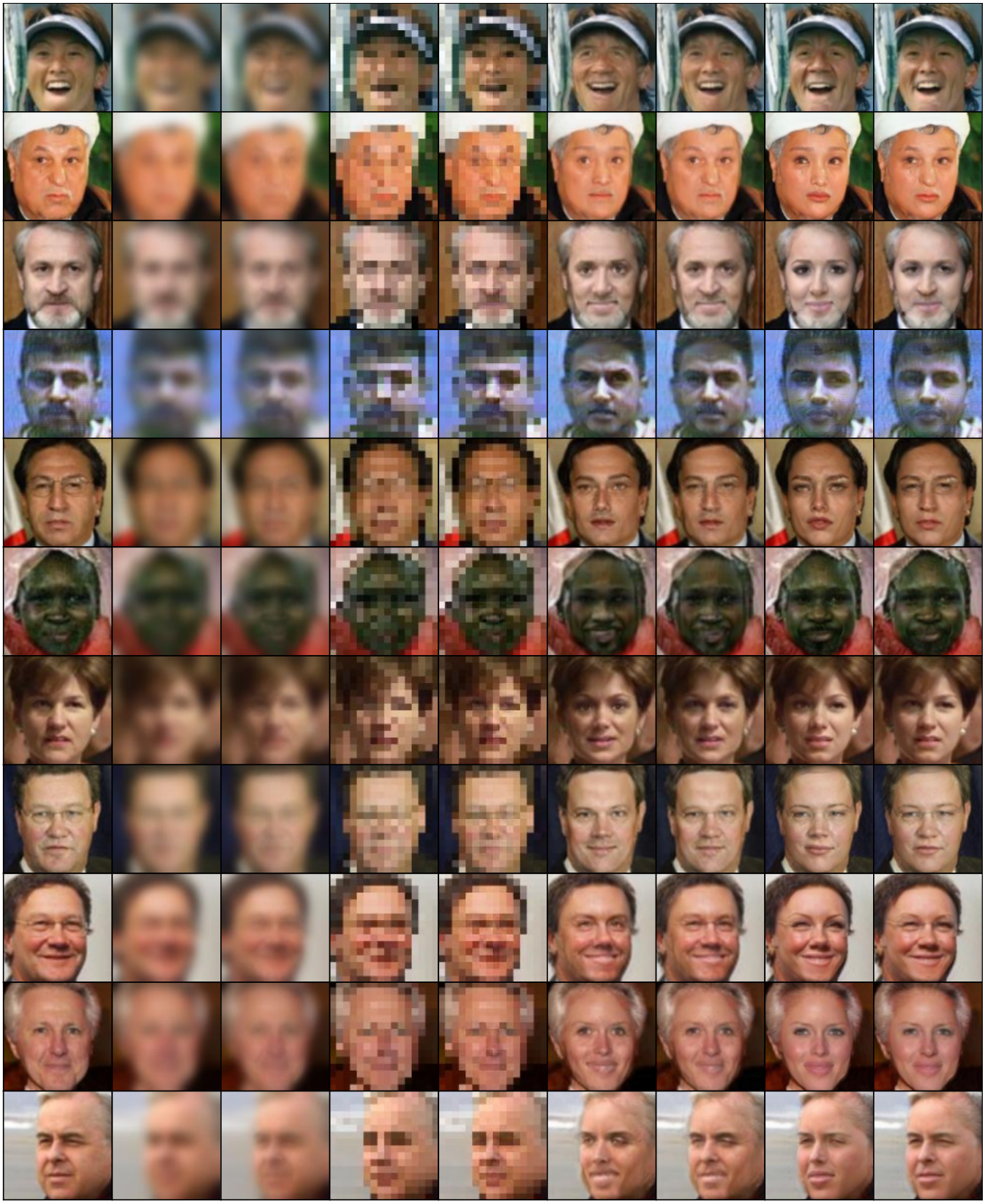

Figure 7: Example images in different protected forms with respect to the face recognizer IResNet100. The symbol ⋆ indicates PRO-Face protected image corresponding to the obfuscation.