

Face Recognition Prevention

Charles Beumier Thibault Debatty
Royal Military Academy, Brussels, Belgium

1. Project F-REC (Face Recognition Prevention)

- ▶ AI now surpasses human capabilities, increasing risks to privacy
- ▶ Large volumes of facial images circulate on social media and the web
- ▶ Civilian and military personnel should be cautious when uploading images
 - Risks for privacy include OSINT exploitation, blackmail, harassment
- ▶ BE MoD/Cylab + Luxembourg Univ. (SnT), 2025-2027

2. WP1 - Accessories Recommendation

- ▶ Impact of scarves, glasses, bandanas, **makeup** ?
- ▶ Much is known from early face recognition studies
- ▶ Bandanas adopted for the National day parade in 2025



Figure 1: Bandanas adopted during parade (21 July 2025)

3. (WP1) Face Painting Contest

- ▶ Evade AI Face Recognition through Face Painting
 - 3 painting styles: 1) Military 2) Stripes 3) Free style
 - 50 RMA students volunteered
- ▶ GDPR compliance:
 - Notice describing the project and participant rights
 - Signed consent required from volunteers
 - Images will not be publicized without consent

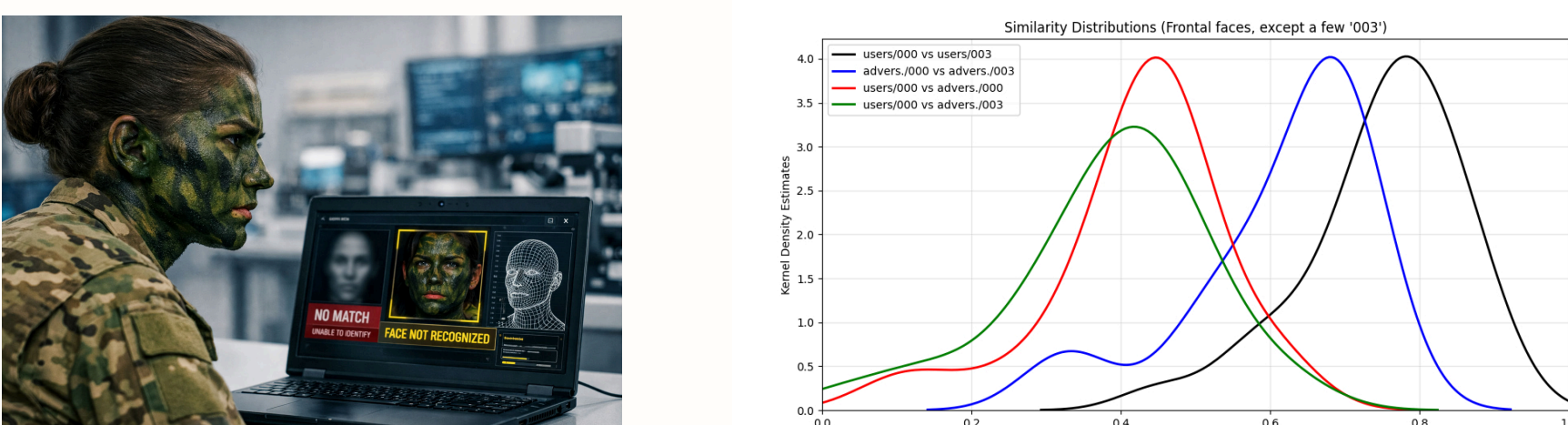


Figure 2: a) Facial camouflage contest b) AI Face similarities (Blue curve: danger recognizing painted vs painted faces)

Acknowledgment

Partner: Univ. of Luxembourg (SnT)
Funding: BE MoD



Generated by Copilot

4. WP2 - AI-based Face Monitoring on Social Media

- ▶ Automatic search for military or civilian faces
- ▶ Scanning social media & web (GDPR constraints !)
- ▶ Access is limited ! (Master Thesis of A. De Groodt)
- ▶ Clearview AI and PimEyes work, but GDPR issues

5. WP3 - Facial Image Modification before Sharing

- ▶ Modify faces in photos to hide identities
- ▶ Applied by the owner, so it requires control
 - Trade-off: Similarity <-> Protection
- ▶ Many approaches: Super-Resolution, Morphing, Swapping

6. (WP3) Super-Resolution

- ▶ 1. Blur faces to hide identifying details
- ▶ 2. Regenerate faces with GFPGAN on blurred faces
 - But little control
 - GANs may introduce artifacts & instability (gaze, pose)

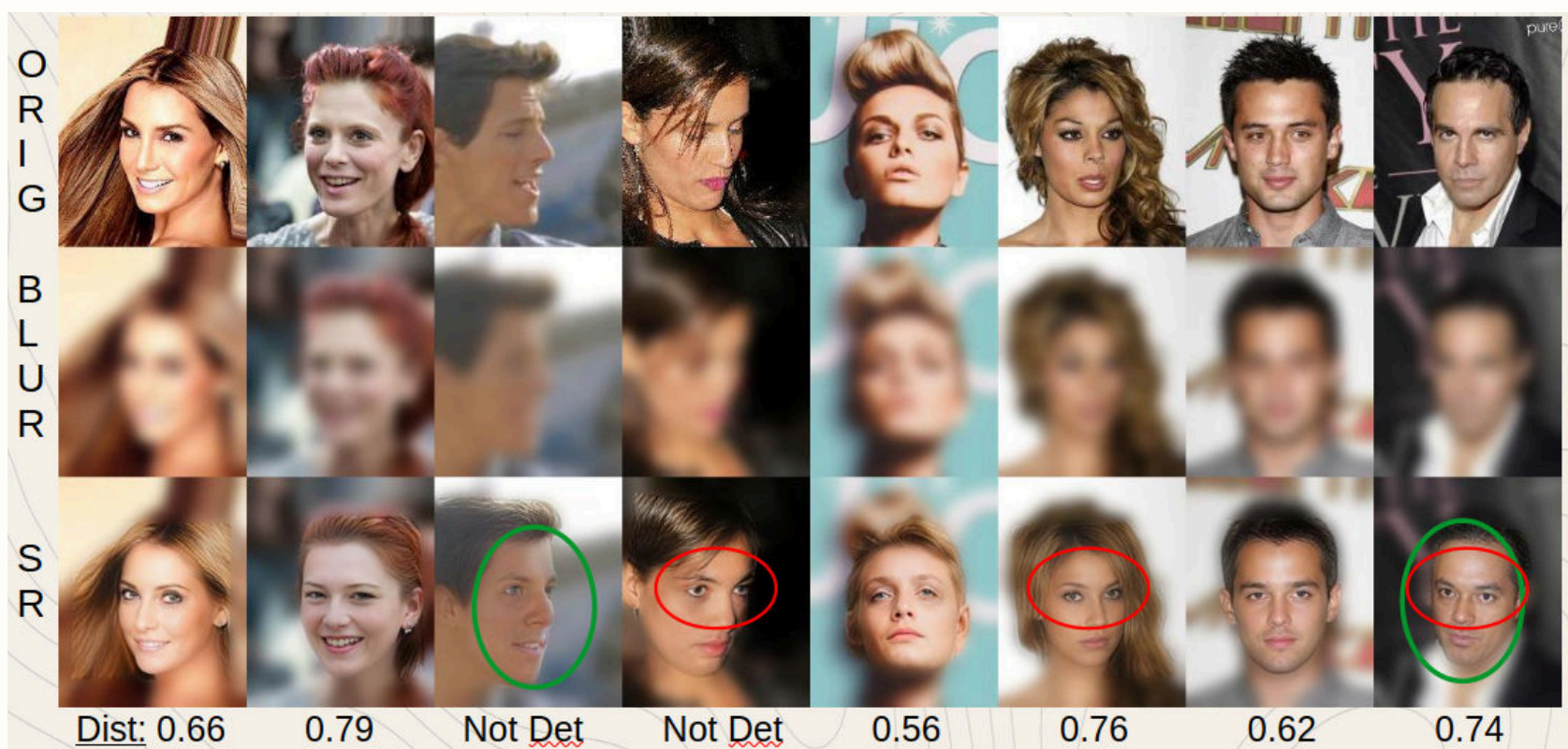


Figure 3: Super-resolution of faces. Artifacts in Pose and Gaze

7. (WP3) Face Swapping

- ▶ Modify inner faces for privacy (de-identification)
- ▶ Integrate new faces into the scene while respecting:
 - Head posture, eye gaze, expression, light reflection
- ▶ 7.1. FaceFusion
 - Very good results, but difficult to automate tests

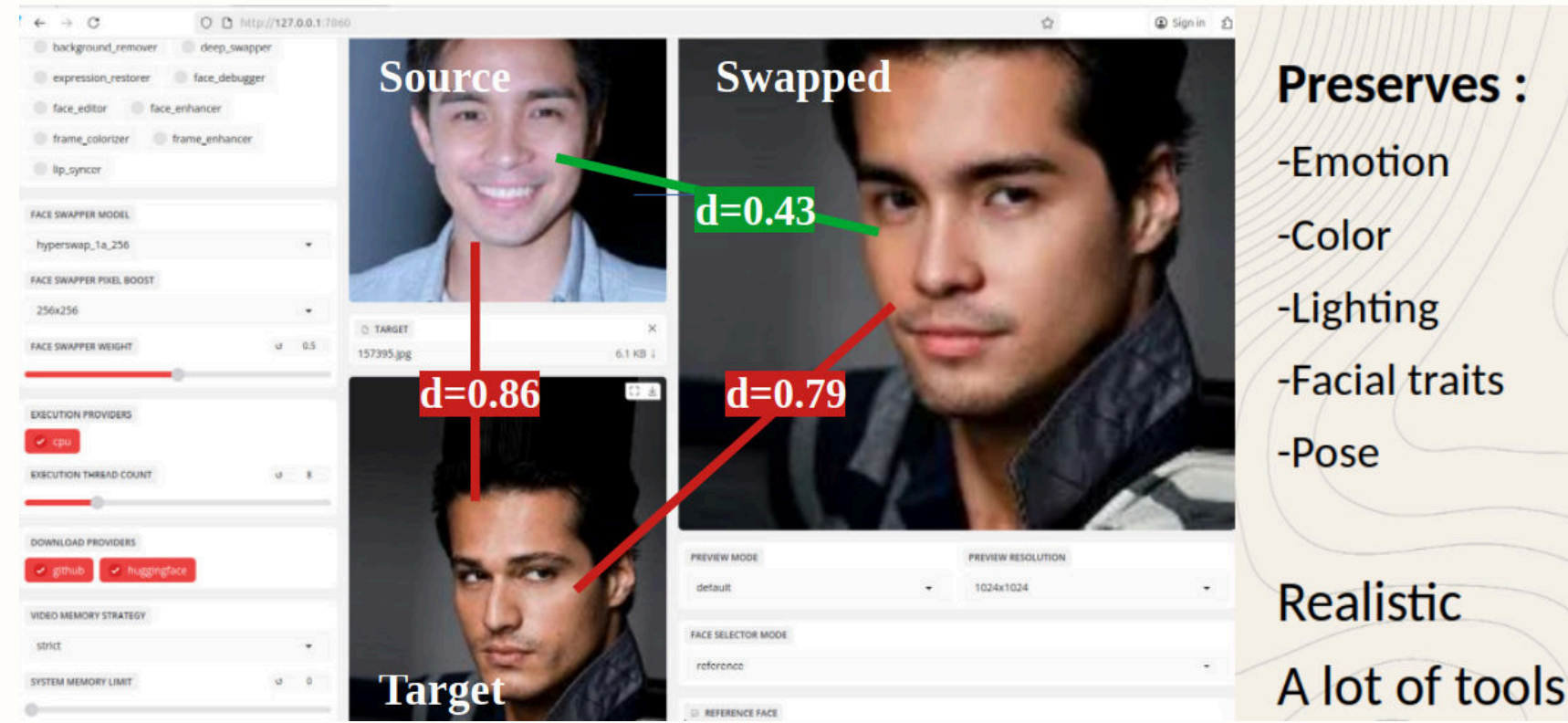


Figure 4: FaceFusion - Source identity transferred to Swapped

- ▶ 7.2. ReActor
 - Very good results, modular design, and automatic testing is possible

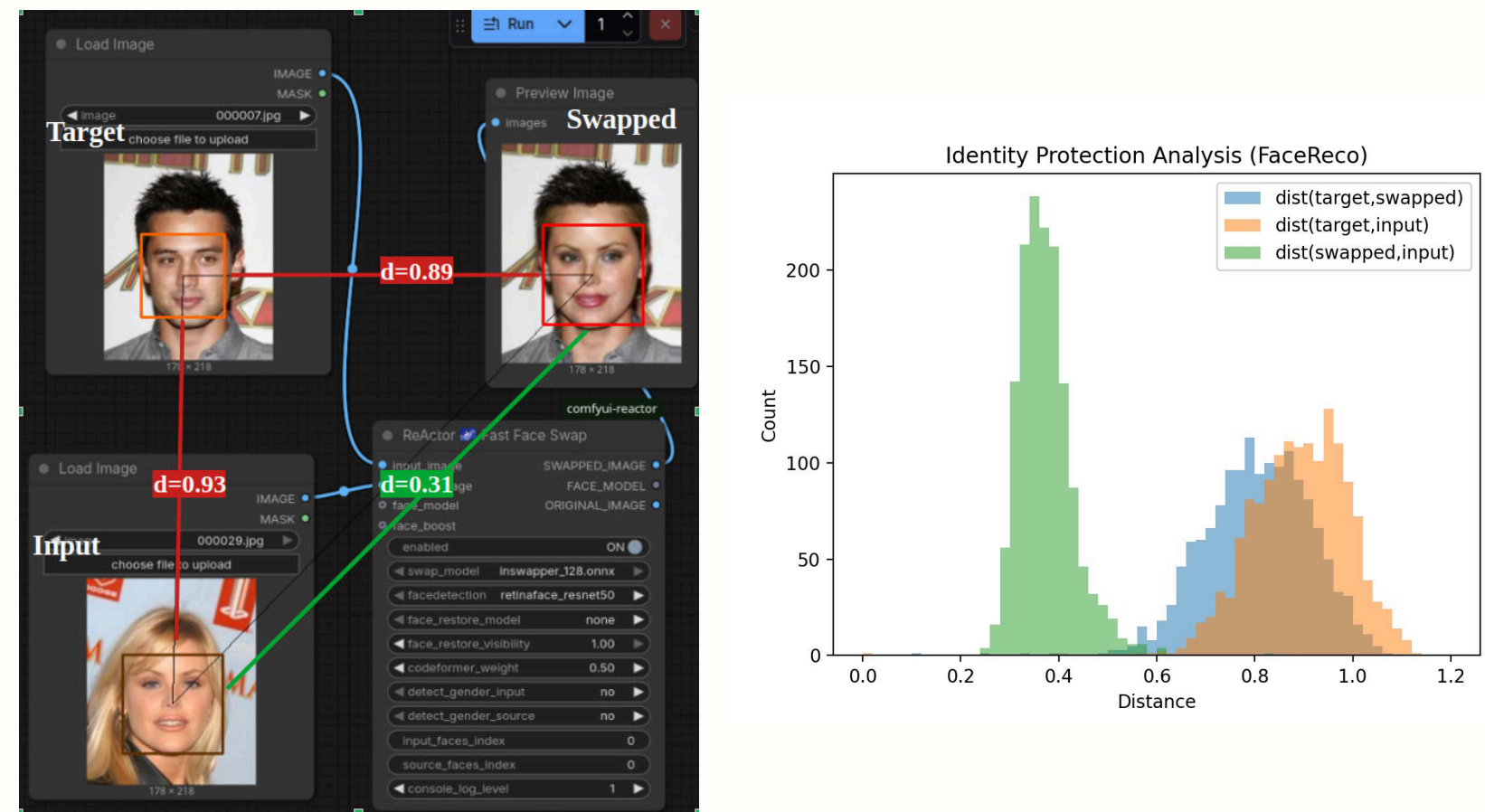


Figure 5: a) Swapping by ReActor b) FR distances on 1500 faces

- ▶ 7.3. InSwapper (from InsightFace)
 - Image-based interface with built-in face detection
 - User selects a replacement identity for each detected face
 - Adequacy check (gender consistency, embedding distance)

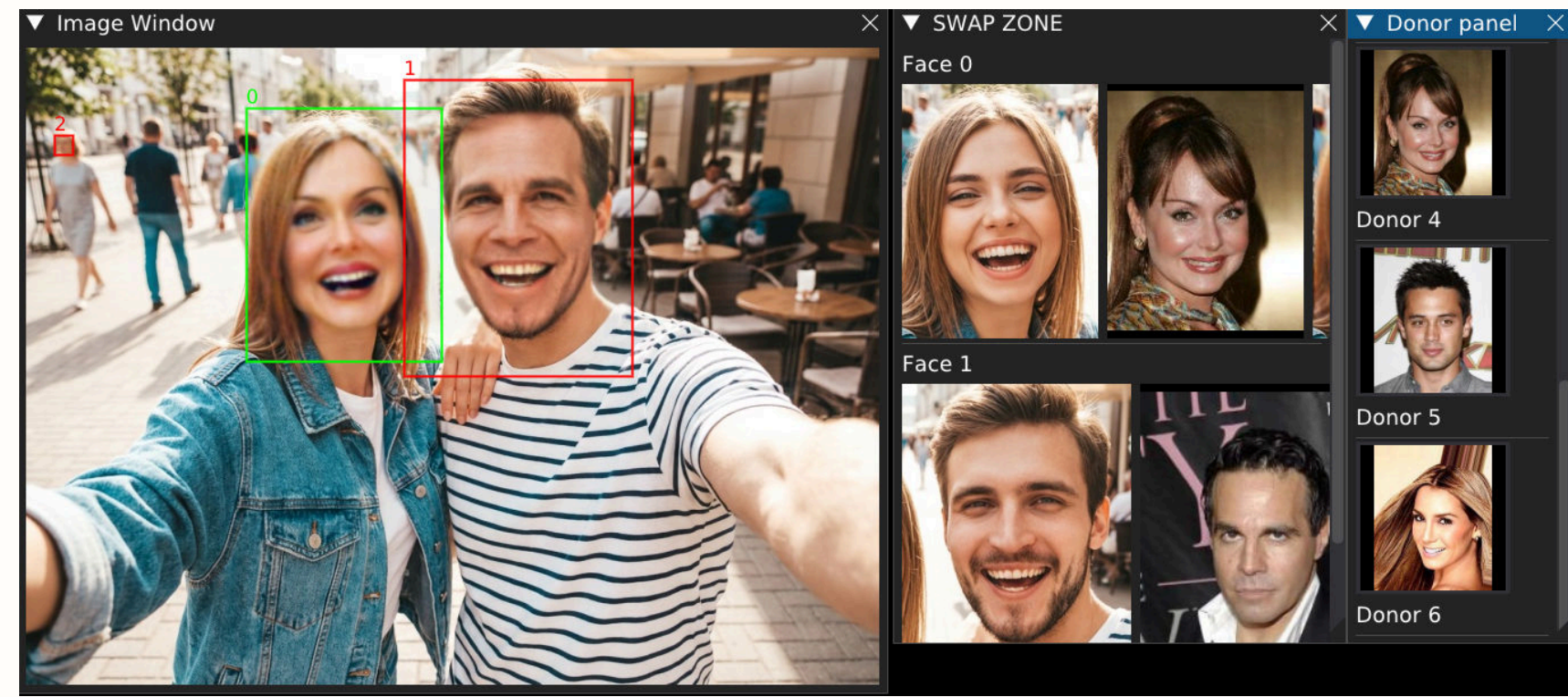


Figure 6: Swapping interface built on InSwapper (InsightFace)

References

- [1] The project "Face Recognition Prevention" is funded by MDN [Jul2025-Dec2027].
- [2] Alexandre De Groodt, "Face Recognition Prevention - Face web scraping", Master Thesis, ULB 2025.
- [3] P. Borsukiewicz, E.-H. Diallo, A. Bonkougou, W. C. Ouédraogo, J. Klein, C. Beumier, and T. F. Bissyandé, "Faces in Focus: Evaluating Generalizability and Transferability of Facial Recognition Explainability Techniques for CNN-based Models," in Proc. of CVPR, Denver, USA, 3-7 June 2026.

