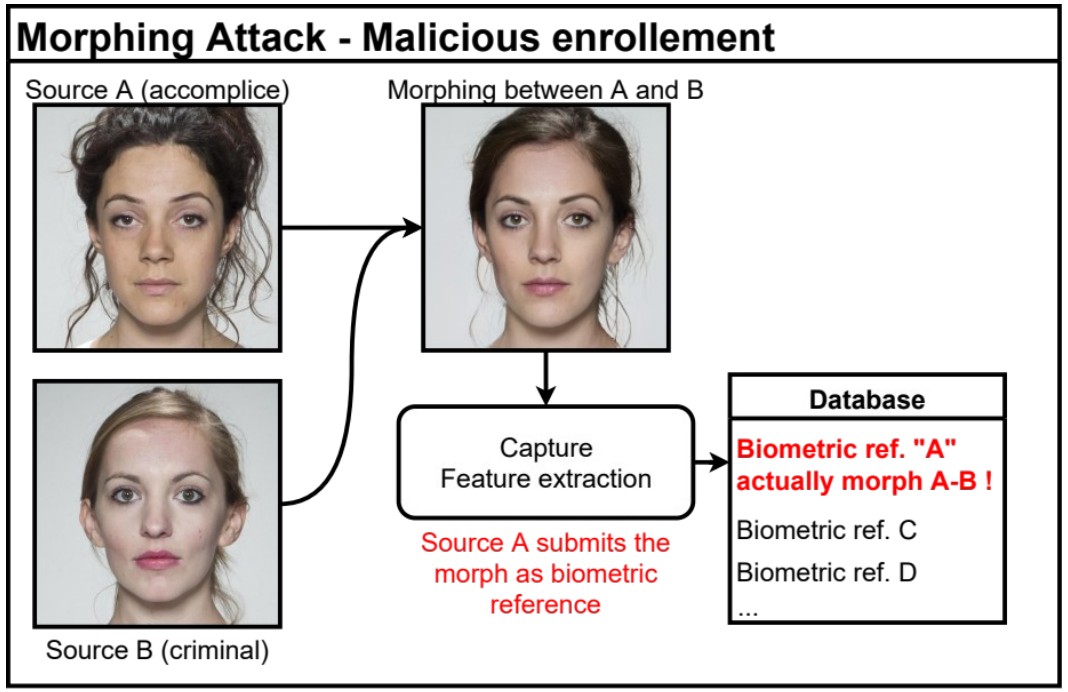
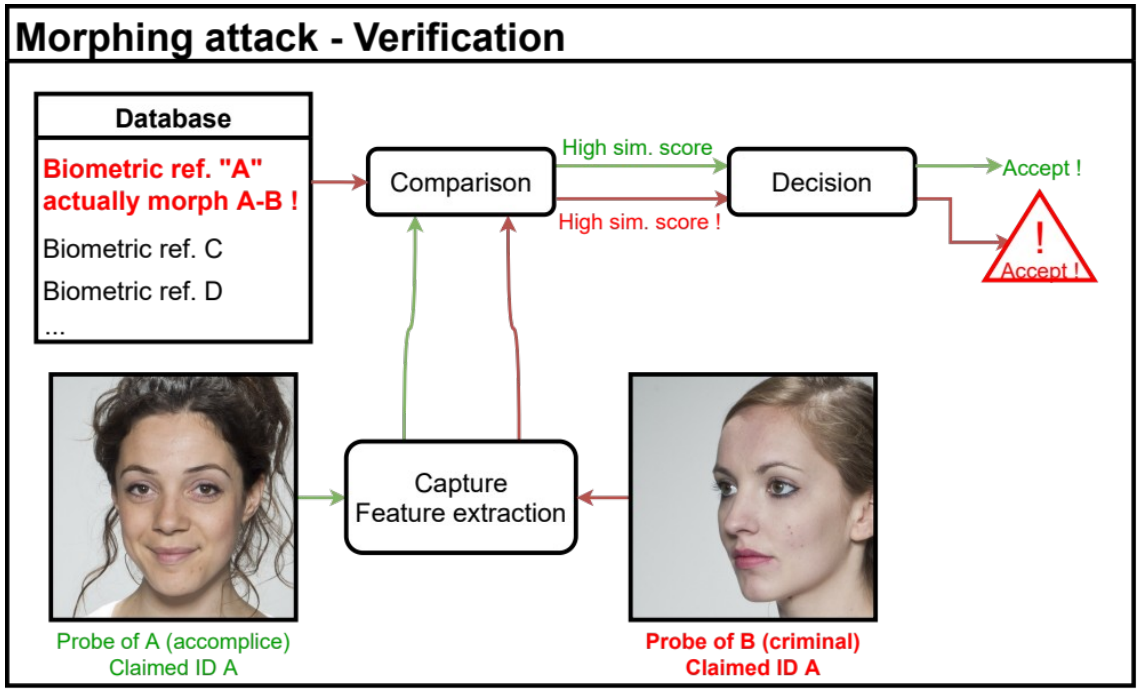
Approximating Optimal Morphing Attacks using Template Inversion

Laurent Colbois

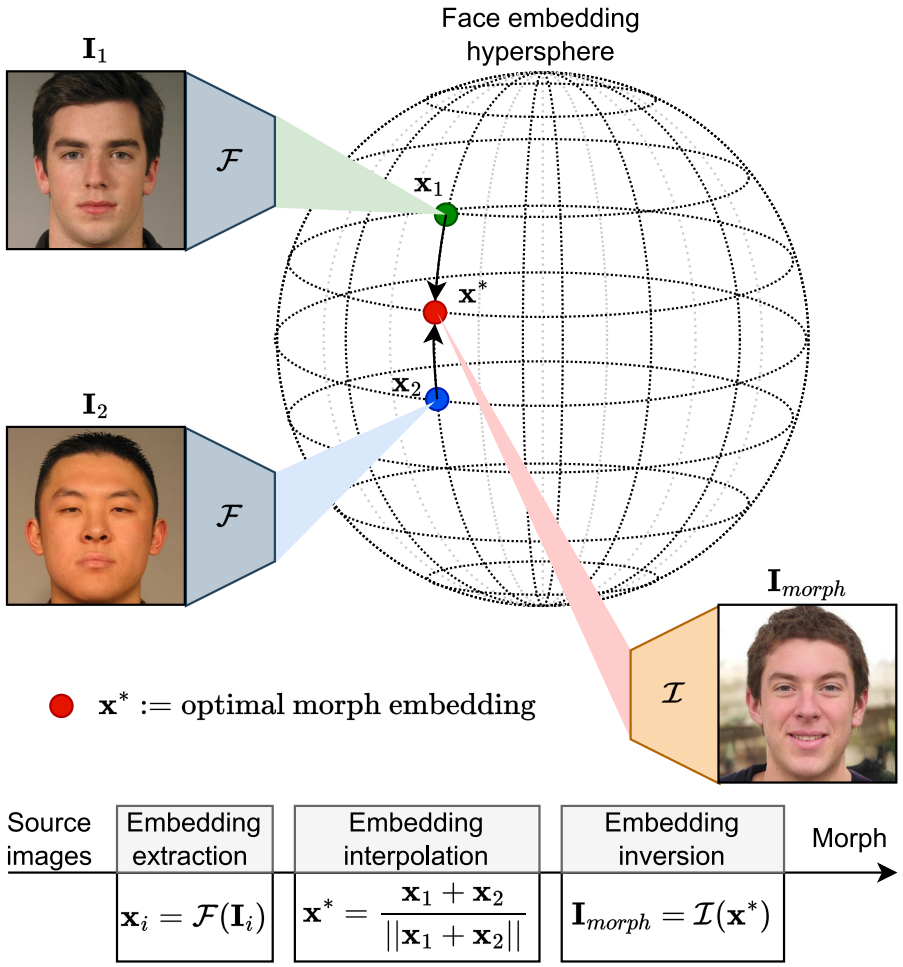
Scenario – An attack on an automated face recognition system





Laurent Colbois, Hatef Otroshi Shahreza, and Sébastien Marcel. 2023. Approximating Optimal Morphing Attacks using Template Inversion. In *IEEE International Joint Conference on Biometrics*.

Generation : inversion of the optimal morph embedding



- 2 inverted FR systems
- 2 inversion methods

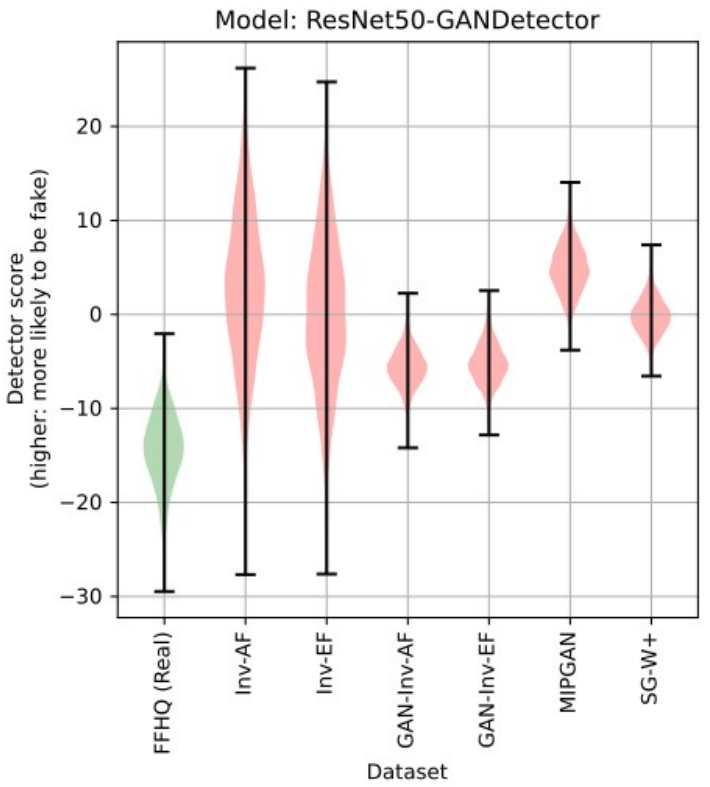
Laurent Colbois, Hatef Otroshi Shahreza, and Sébastien Marcel. 2023. Approximating Optimal Morphing Attacks using Template Inversion. In *IEEE International Joint Conference on Biometrics*.

Evaluation of the morphing method

Vulnerability analysis

FRS	Attack	MinMax-MMPMR (%)	ProdAvg-MMPMR (%)
AF	□ MIPGAN	73.22	54.77
	□ Inv-AF	**89.88**	**74.76**
	□ GAN-Inv-AF	42.76	22.81
	■ SG-W	4.32	1.44
	■ SG-W+	60.10	39.97
	■ Inv-EF	**79.65**	**61.46**
	■ GAN-Inv-EF	16.46	5.85
EF	□ Inv-EF	**87.78**	**74.58**
	□ GAN-Inv-EF	28.88	14.52
	■ SG-W	10.19	3.56
	■ SG-W+	67.63	48.90
	■ MIPGAN	**75.80**	**60.10**
	■ Inv-AF	75.09	58.25
	■ GAN-Inv-AF	28.20	14.73

Detectability



- Inv is more effective against FR systems. Limitations in realism.
- GAN-Inv is not there yet but more realistic, and challenging to the detectors
- Future work
  - Comparison to non-deep methods
  - Print-scan
  - Morph fine-tuning

Laurent Colbois, Hatef Otroshi Shahreza, and Sébastien Marcel. 2023. Approximating Optimal Morphing Attacks using Template Inversion. In *IEEE International Joint Conference on Biometrics*.

idiap RESEARCH INSTITUTE