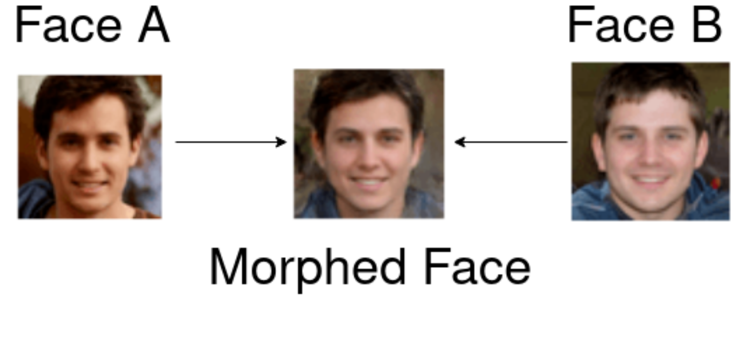
Leveraging Adversarial Learning for the Detection of Morphing Attacks

Zander W. Blasingame, Dr. Chen Liu

IJCB 2021

Department of Electrical and Computer Engineering
Clarkson University
10 Clarkson Ave, Potsdam NY, 13676, USA

Problem



Problem

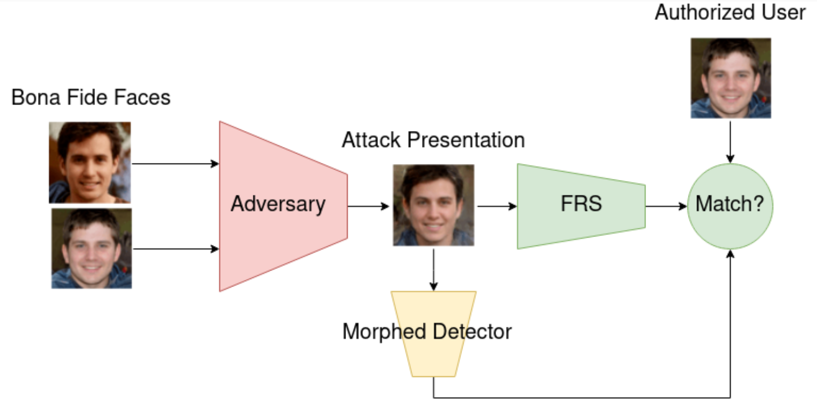
Morphed Attack poses great security concerns

Description

Fool FRS into accepting **two** identities as **one**

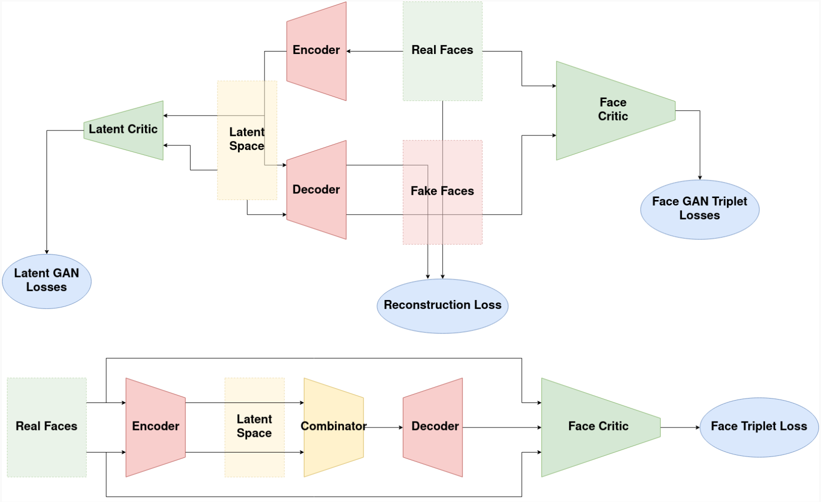
Leverage Adversarial Formulation

Adversarial Structure



Use GAN architecture to train detector

Proposed Architecture



Datasets

- FERET
- Face Research Lab London (FRLL)

Morphs

- StyleGAN2 (deep learning based)
- FaceMorpher (landmark based)
- OpenCV (landmark based)

Experiments

- Each permutation of training and testing, dataset and morph
- 36 unique experiments per detector repeated 10 times

Results

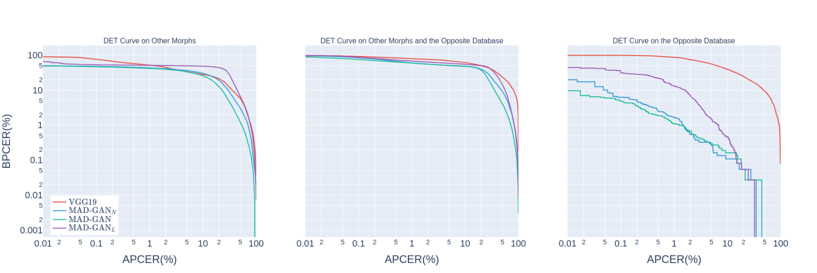


Figure 1: Summary DET curves.

Summary

- Created novel detection algorithm leveraging the adversarial structure
- Evaluated with extensive experiments using different combinations of morphs and experiments.