Morphing Attack Detection

Una M. Kelly

Datamanagement and Biometrics, University of Twente

What are Morphing Attacks?

A *morph* is an image that contains facial features of two different people. In a border-crossing scenario a criminal could enlist the help of an accomplice to create a morphed photo. The accomplice could then use this photo to apply for a passport, which the criminal in turn could use to cross borders undetected. The most-used method to create morphs is to mark certain facial features, called landmarks, warp both images to a common geometry and then blend the pixel values.

Figure 1:Two genuine facial images.

Figure 2:The two images from Fig. 1 morphed. Since the background was included *ghosting artifacts* are visible.

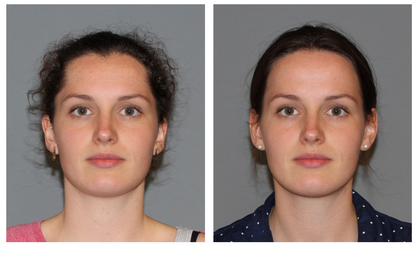

Figure 3:The morph from Fig. 2 spliced into the first background (left) and spliced into the second background (right).

Objectives

To reduce the threat posed by morphing attacks we can:

- Generate different types of morphs. These can be used to train and evaluate morphing attack detection methods.
  - Currently mostly landmark-based morphs are used in research, which can lead to overfitting of detection methods and underestimation of the vulnerability of face recognition systems.
- Improve morphing attack detection methods.
  - We focus on developing detection methods that generalise well, i.e. are robust to unknown types of morphing attacks.

New Morphing Methods

- We introduce the theoretical concept of **worst-case morphs** [1], which are those morphs that are most challenging for a fixed face recognition (FR) system. We generate images that approximate such worst-case morphs by treating the FR system as the Encoder in an Autoencoder and training a Decoder to map from the FR latent space back to image space.
- Combining Variational Autoencoders (VAE) and Generative Adversarial Networks (GAN) enables interpolation between real images. We improve an existing method to generate morphs by incorporating advantages of Wasserstein GANs, resulting in more stable training. This enables us to generate morphs with higher resolutions. See Fig. 4.

Figure 4:The images in the middle column are morphs generated from the real images on the left and right using a combination of VAE and GAN.

Detecting Morphs

- If a reference image is available, **demorphing** can be applied to a potential morph in order to reverse the morphing process and retrieve the identity of the accomplice. Instead of demorphing in image space, we apply demorphing **in latent space**. The FR latent embeddings of the two images are needed to compute a (dis)similarity score anyway, so applying demorphing to the latent embeddings instead of the images requires fewer computations. Furthermore, a network to visualise the results of demorphing can be added, but this is not necessary.

Morphing-Robust Face Recognition

- Instead of focussing on morphing detection methods we can also try to make FR systems themselves more robust to morphing attacks. In [2], we attempt to improve deep learning-based face recognition simply by treating morphed images just like real images during training.

Latent Spaces

- We found that the way we examine images in the latent space of an FR system (for generating worst-case morphs or for demorphing in latent space) has other uses too! We developed a method to slightly change images so that visually they appear unchanged, but a FR system cannot recognise the identity anymore. See Fig. 5. This approach can be used to protect privacy.

Figure 5:Visually the two images in each pair look very similar, but according to a FR system they have different identities.

References

[1] U.M. Kelly, L.J. Spreeuwers, and R.N.J. Veldhuis. A face recognition system's worst morph nightmare, theoretically. *CoRR*, abs/2111.15416, 2021.

[2] U.M. Kelly, L.J. Spreeuwers, and R.N.J. Veldhuis. Improving deep-learning-based face recognition to increase robustness against morphing attacks. In *Computer Science & Information Technology (CS & IT)*. AIRCC Publishing Corporation, December 2020.

Contact Information

Are you interested in this research? Would you like to do a Bachelor or Master assignment on a morphing-related topic? Email me at u.m.kelly@utwente.nl !