GAN output: Which are real, which are fake?
GAN output: Which are real, which are fake?

What is a GAN?

“Wasserstein GAN” (2017)  
Arjovsky, Chintala, Bottou

To train D minimise:

$$L_D = \frac{1}{N} \sum_{i=1}^{N} D(x_i) - D(G(v_i)) + "GP\ term"$$

To train G minimise:

$$L_G = \frac{1}{N} \sum_{i=1}^{N} D(G(v_i))$$

E.g. “Improved Training of Wasserstein GANs” (2017), Gulrajani, ..., Courville
1. Do GANs generate new identities?
   • Applications: Dataset-anonymisation; semi-supervised learning with distractor images

2. Can GAN Images be used in Biometric Systems?
   • Applications: Non-regression tests; Performances extrapolation; Algorithm-improvement evaluation; Data-augmentation with synthetic sets of mated images …
1. Do GANs generate new identities?
Typical qualitative analysis of overfitting

Visual, nearest-neighbour analyses are typically performed…

Synthetic images:

Nearest neighbours in VGGNet feature-space:

Images taken from Karras et al. (2018)

• What about the rest of the space? How frequently do look-alikes occur?
Assessing the frequency of look-alikes (Nearest neighbors)

Matching scores generated using a recent biometric network

All Matching scores

Nearest neighbors scores

ProGAN: Progressive Growing of GANs for Improved Quality, Stability, and Variation. T.Karras & All, ICLR. 2018
StyleGAN: A style-based generator architecture for generative adversarial networks. T.Karras & All, CVPR. 2019
2. Can we use synthetic images as distractors?
Performances with real and fake distractors

- Synthetic images can be used as distractors to estimate performance with real data.
- As images from GANs exhibit less variability, extrapolation for very large datasets is still uncertain.
3. Can we generate multiple images of the same fake identity?
The “InterFaceGAN” method manipulates attributes by traversing the GAN’s latent space in the direction perpendicular to a particular decision boundary.
IVI-GAN, Marriott et.al. (arxiv 2018 – FG 2020)
SD-GAN, Donahue et.al. (2018)

\[
\mathcal{L}_{\theta_D} = D(x) - D(G(z_1), G(z_2)) \\
\mathcal{L}_{\theta_G} = D(G(z_1), G(z_2))
\]
SD-GAN + Triplet loss, Marriott et.al. (IJCB 2020)

\[ \mathcal{L}_{\theta_D} = D(x) - \frac{1}{2}[D(G(z_1), G(z_2)) + D(\bar{x})] \\
+ \lambda[D(G(z_1), G(z_2)) - D(\bar{x})]^2 \\
\mathcal{L}_{\theta_G} = D(G(z_1), G(z_2)) \]
Disentangled Datasets

- InterFaceGAN (CelebA-HQ)
- IVI-GAN (CelebA)
- SD-GAN (Mugshots)
- SD-GAN + Triplet (Mugshots)
4. Can GAN Images be used in Biometric Systems?
Biometric scores for mated pairs

Matching score distributions within mated sets, with default parameters

- Mated pairs of synthetic images can be used to compute biometric scores.
- Scores are higher for imposter tests with GAN images.
- Identities are not so well disentangled from other attributes.
- All methods have explicit or implicit parameters leading to different intra-class variability.
Biometrics Evaluation of GANs

SD-GAN + **Triplet loss**

- **Z_{IV}** is a Gaussian random vector controlling the intra-class variability.

- GANs can be tuned to adjust intra-class variability, in order to reach desired biometric performances.

![Graph showing biometric evaluation with various standard deviations for intra-class distributions.](image-url)
• Most improvements in biometric algorithms can be seen on synthetic datasets.
Conclusions

1. Overfitting is *not* occurring. New IDs *are* being generated.

2. Synthetic images allow wider system tests than with the replication of a small dataset.
   - Without privacy concerns
   - Non-regression test, speed test, loading test …
   - Moderate control of pose, illumination, age, glasses and gender distributions

3. Synthetic Images can be used to compute some biometric performances.
   - Behaviour with larger gallery
   - Comparison of different algorithms

4. Today, none of the assessed methods was able to fully disentangle identity. It is still a research topic.
   - Not yet ready to be used as training datasets for biometric algorithms
Questions ?

stephane.gentric@idemia.com
References

**Deng et.al. (2019)**

**Donahue et.al. (2018)**

**Karras et al. (2018)**

**Marriott et.al. (2020)**

**Shen et al. (2020)**

**Marriott et.al. (2020)**