

# **Autoencoders and Generative Adversarial Networks**

Giacomo Boracchi

Advanced Neural Networks and Deep Learning

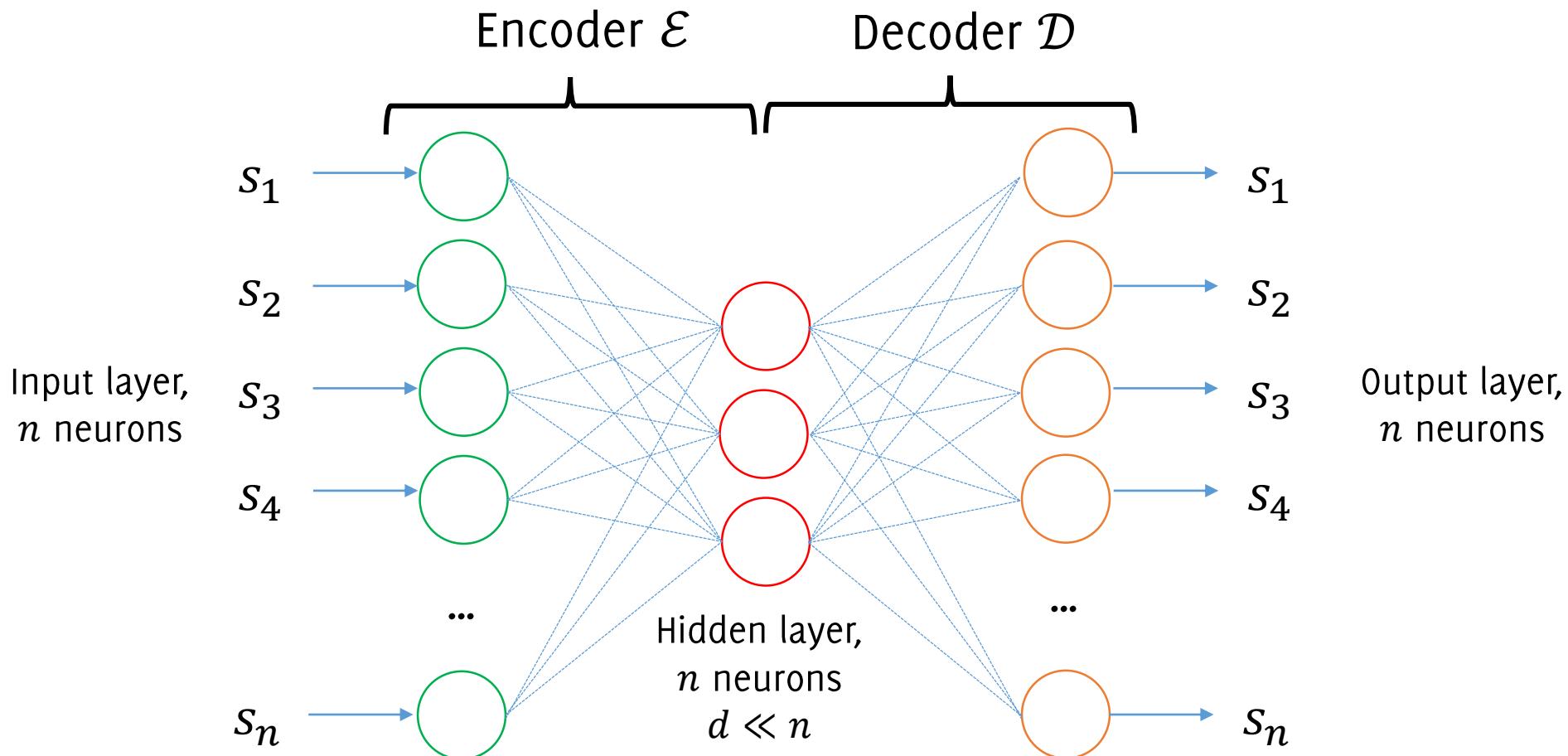
<https://boracchi.faculty.polimi.it/>

# Autoencoders

# Autoencoders using MLP

Autoencoders are neural networks used for data reconstruction (unsupervised learning)

The typical structure of an autoencoder is:



# Autoencoders using MLP

Autoencoders can be trained to reconstruct all the data in a training set.

The reconstruction loss over a batch  $S$  is

$$\ell(S) = \sum_{s \in S} \|s - \mathcal{D}(\mathcal{E}(s))\|_2$$

and training of  $\mathcal{D}(\mathcal{E}(\cdot))$  is performed through standard backpropagation algorithms (e.g. SGD).

The autoencoder thus learns the identity mapping.

**Rmk** there are **no external labels** involved in training the autoencoder, as it performs reconstruction of the input

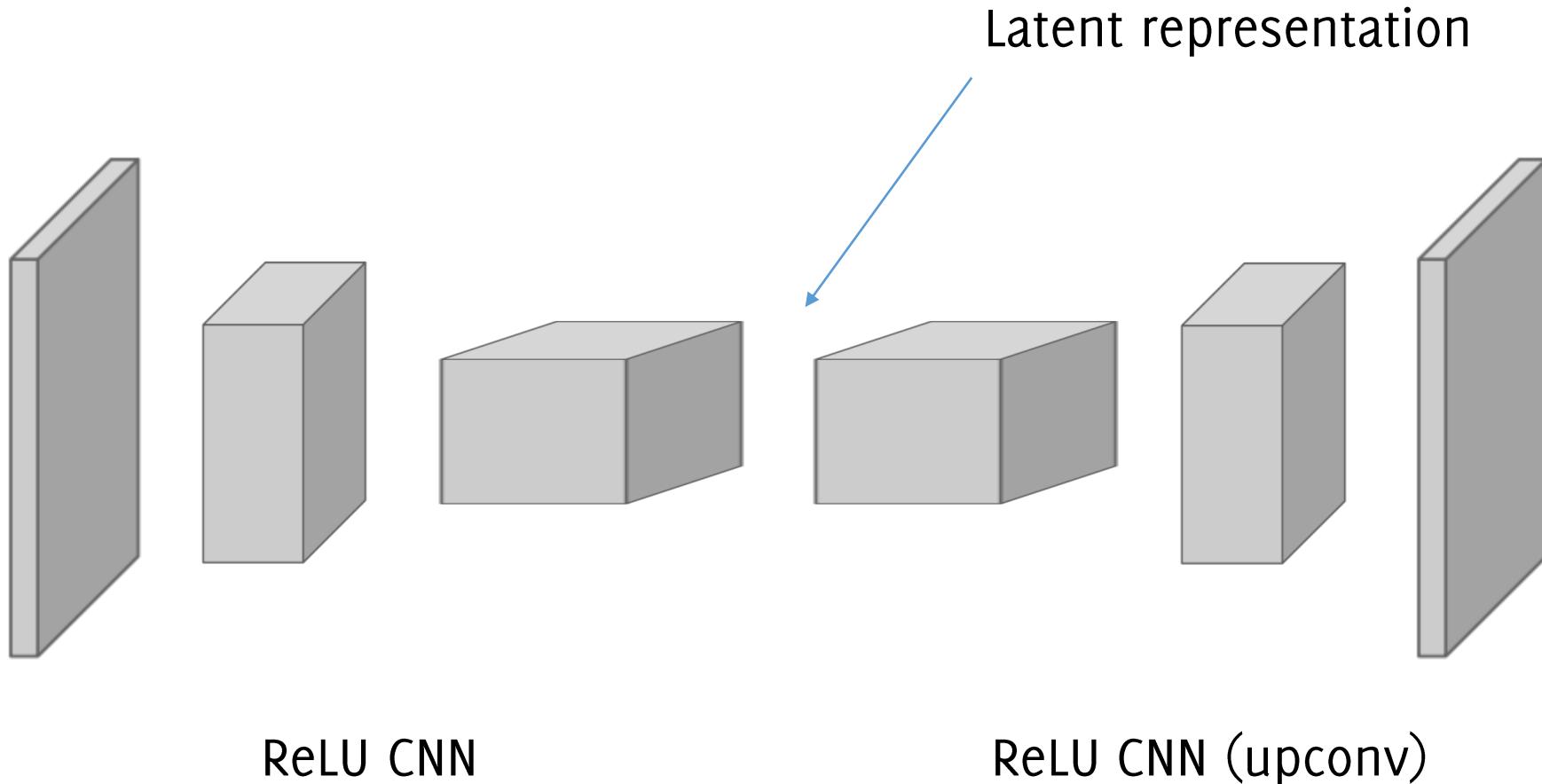
# Autoencoders

## Remark:

- Features  $z = \mathcal{E}(s)$  are typically referred to as **latent representation**
- AE typically do not provide exact reconstruction since  $n \ll d$ , by doing so we **expect the latent representation to be a meaningful and compact representation** of the input
- **It is possible to add a regularization term**  $+ \lambda \mathcal{R}(s)$  to steer latent representation  $\mathcal{E}(s)$  to satisfy desired properties (e.g. sparsity) or the reconstruction  $\mathcal{D}(\mathcal{E}(s))$  (e.g. smoothness, sharp edges in case of images)
- More powerful and nonlinear representations can be learned by **stacking multiple hidden layers** (deep autoencoders)

# Convolutional AutoEncoders

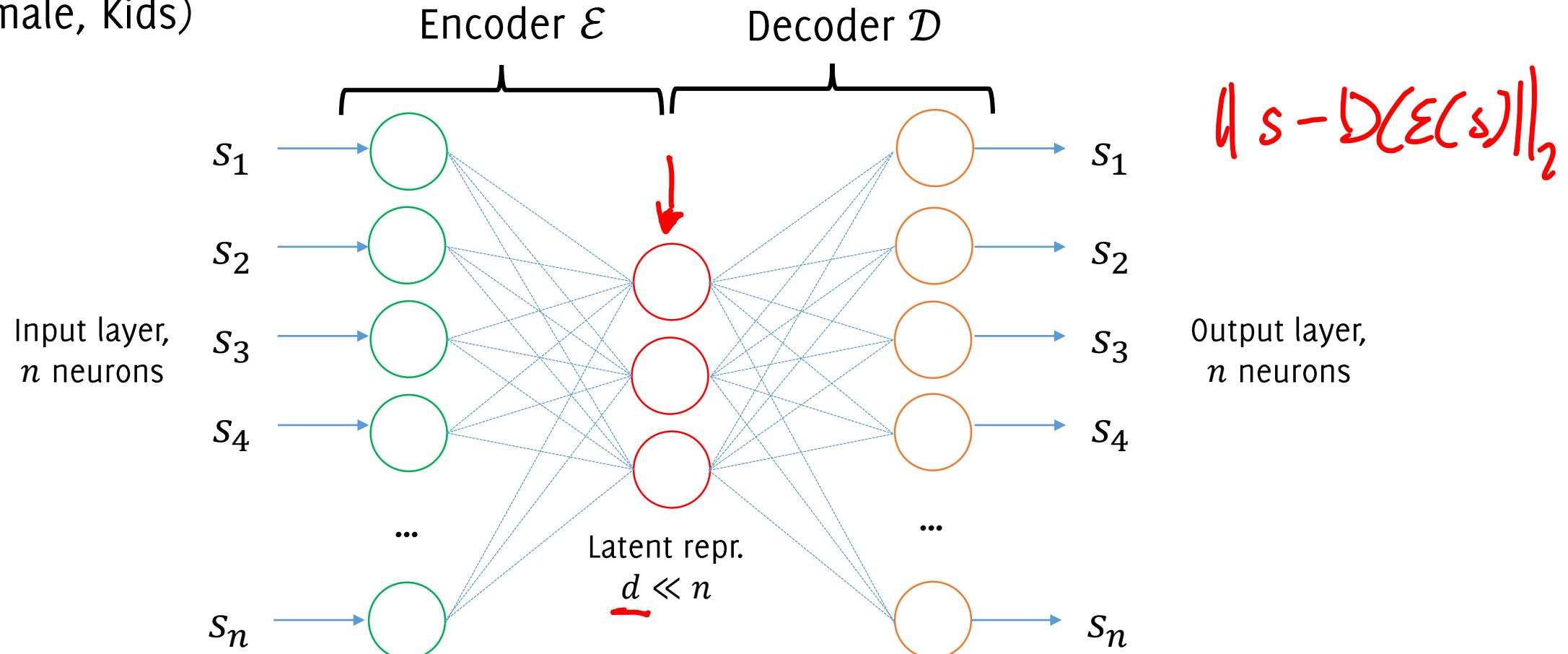
And of course it is possible to use convolutional layers and transpose convolution to implement a deep convolutional autoencoder



# Using Autoencoders for classifier initialization

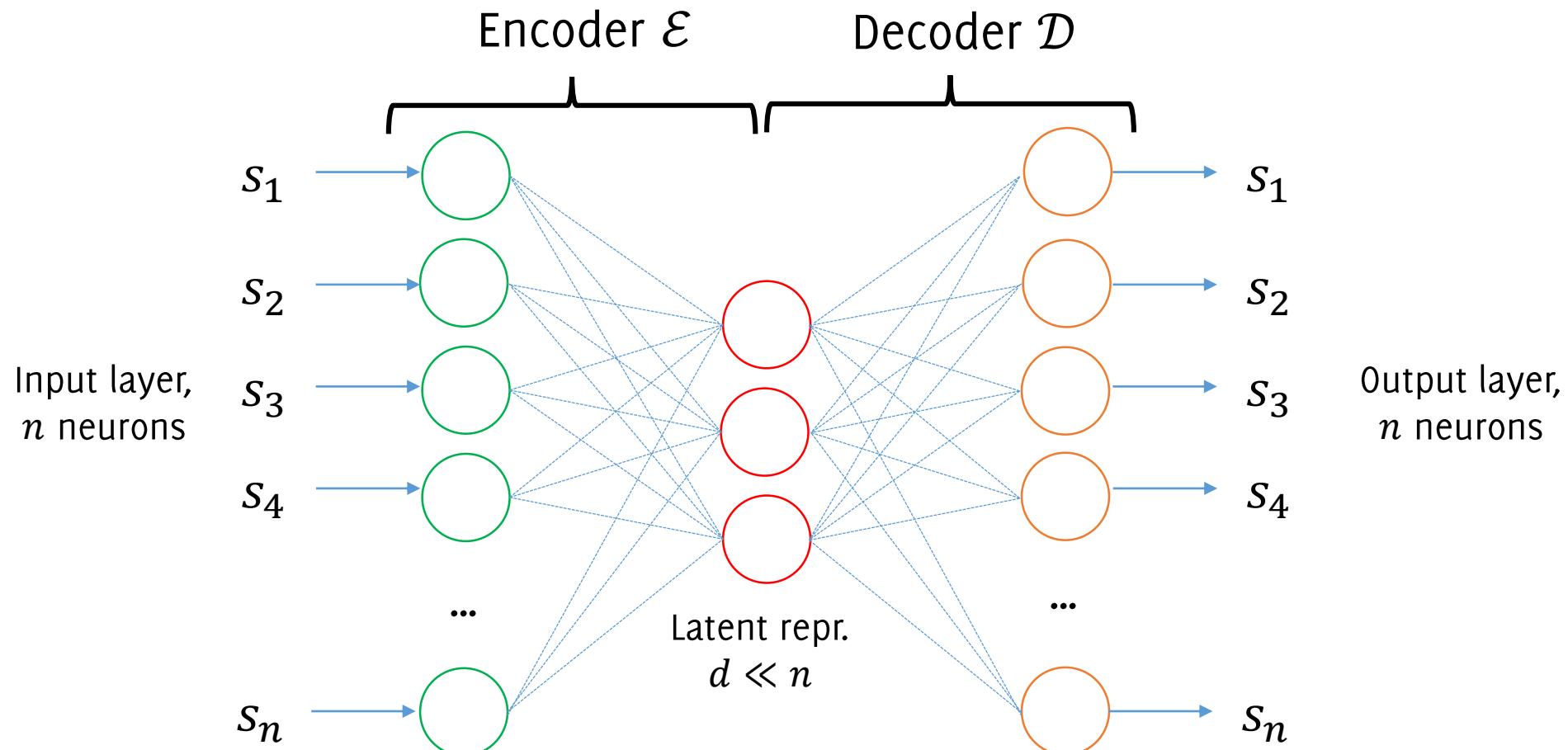
Autoencoders can be used to **inizialize the classifier** when the training set includes

- **few annotated data** (e.g. a large set  $S = \{s_i\}$  of unlabeled human faces)
- **many unlabeled ones** (e.g. a small set  $L = \{(s_i, y_i)\}$  of faces labelled as Male, Female, Kids)



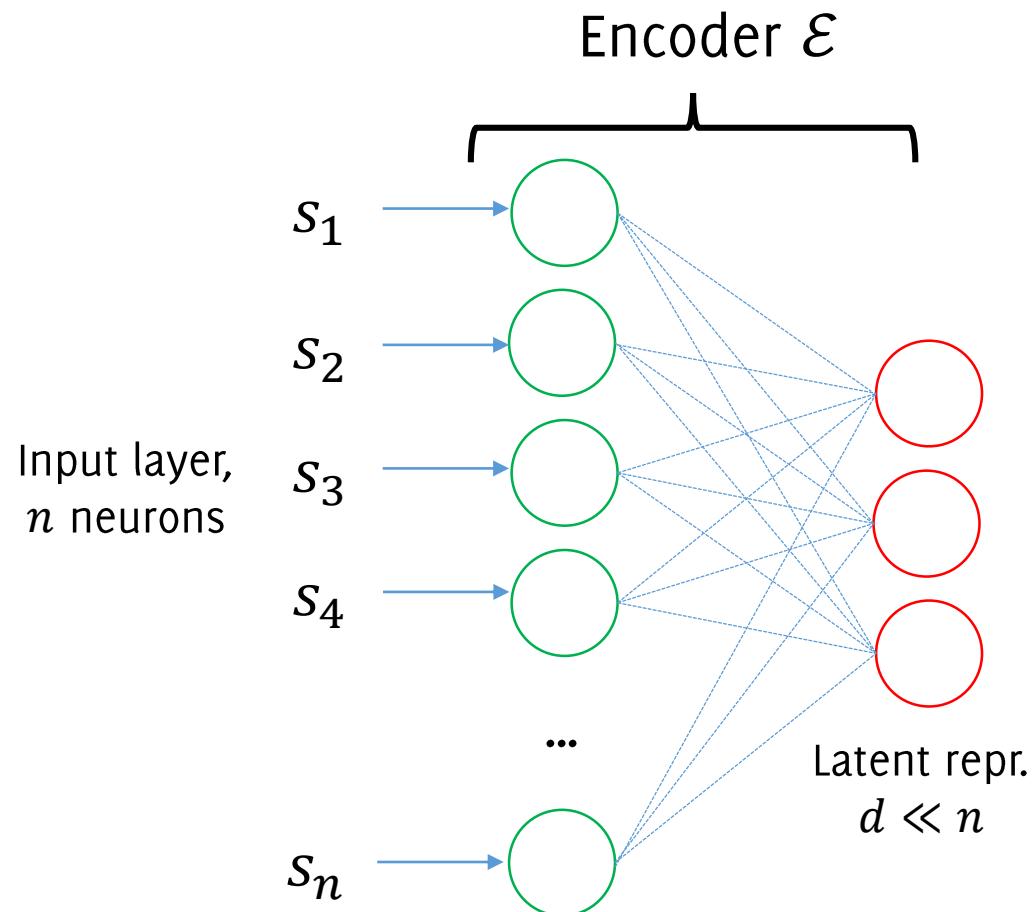
# Using Autoencoders for classifier initialization

- 1) Train the autoencoder in a fully unsupervised way, using the unlabeled data  $S$



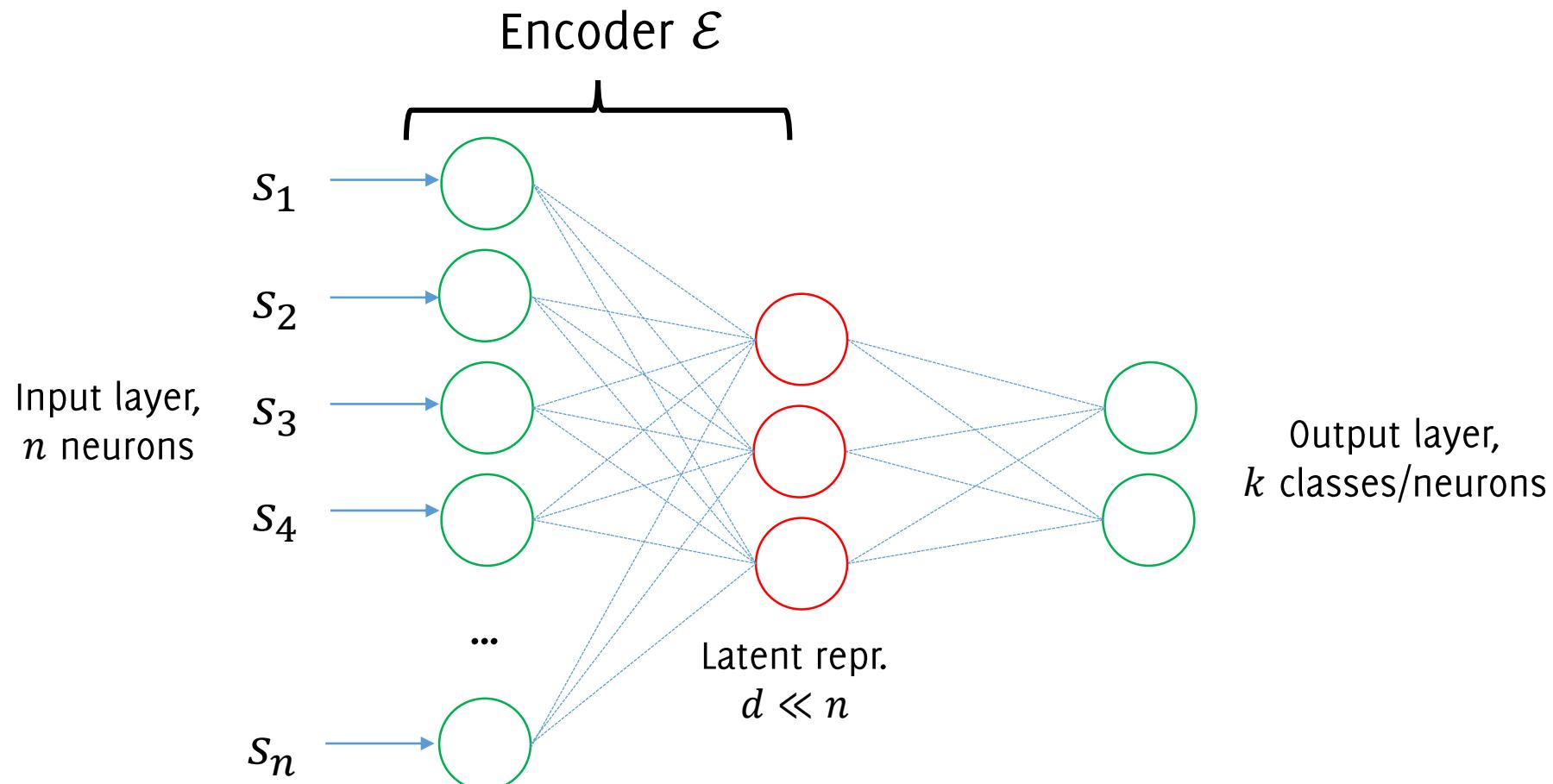
# Using Autoencoders for classifier initialization

2) Get rid of the decoder and keep the encoder weights



# Using Autoencoders for classifier initialization

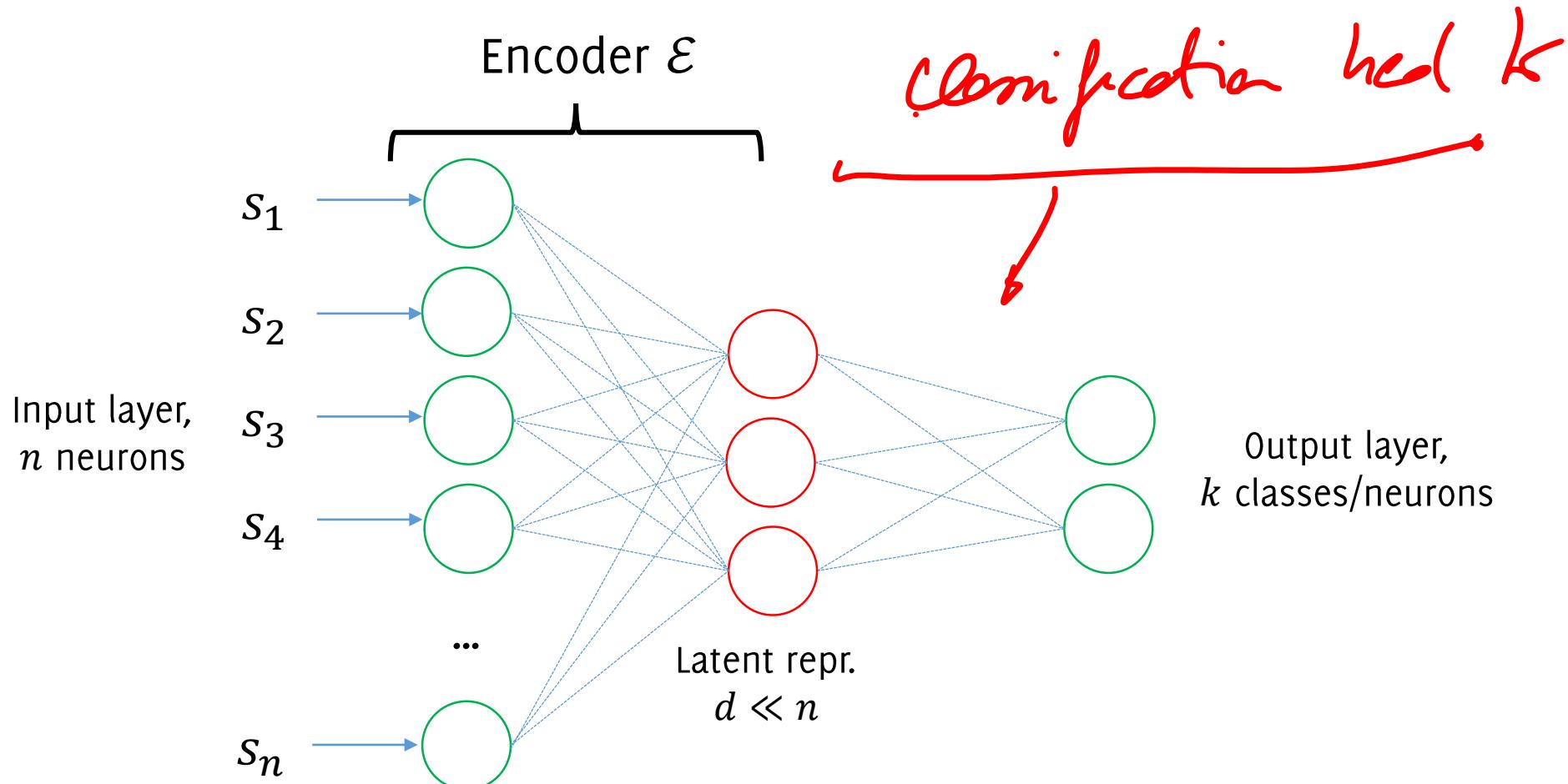
3) Plug in a FC layer for classifying samples from the latent representation



# Using Autoencoders for classifier initialization

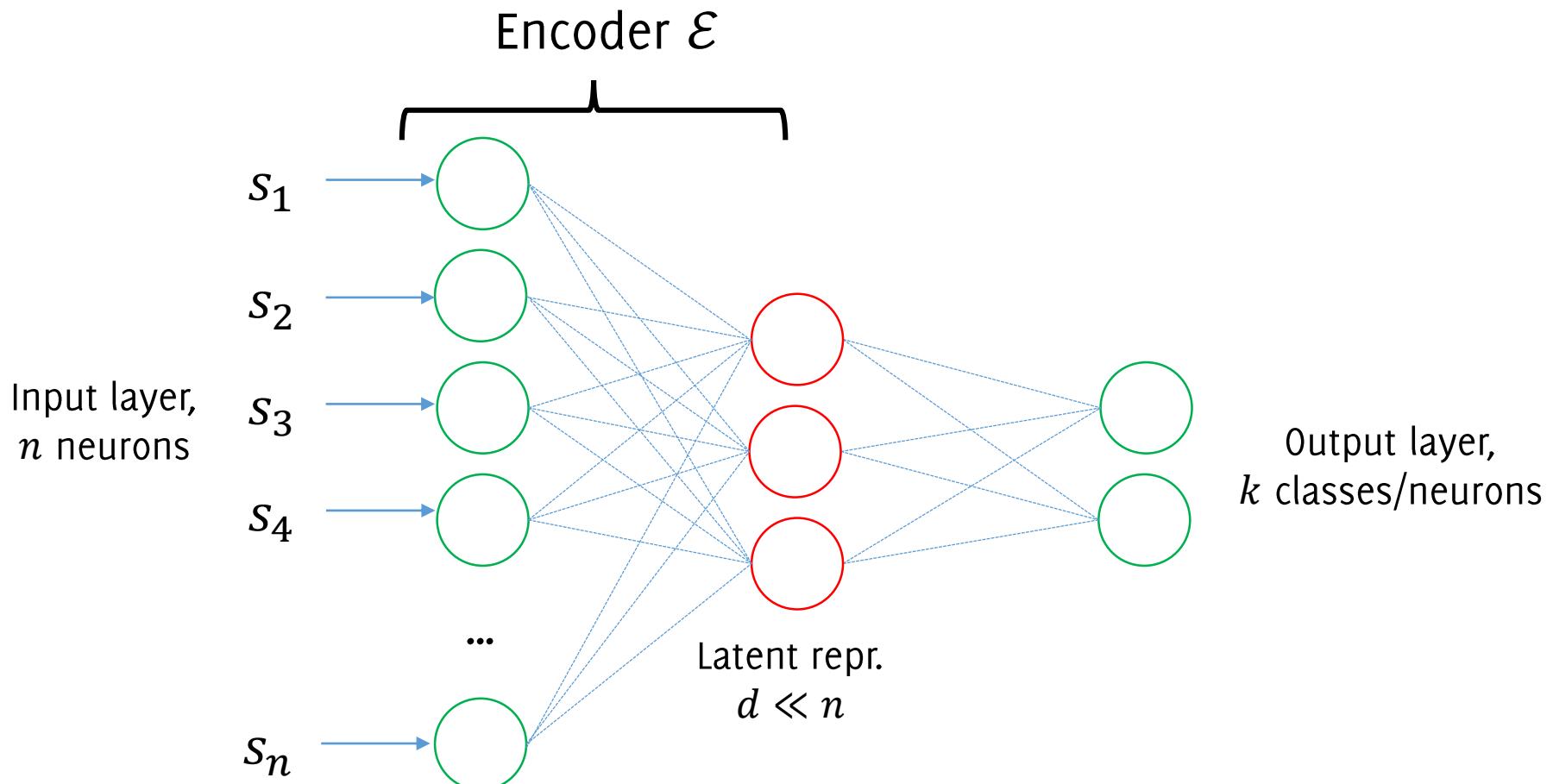
4) Fine tune the autoencoder using the few supervised samples provided  $L$ . This is perfectly in line with «Transfer Learning» and holds for whatever model.

If  $L$  is large enough, the encoder weights  $\mathcal{E}$  can also be fine-tuned



# Using Autoencoders for classifier initialization

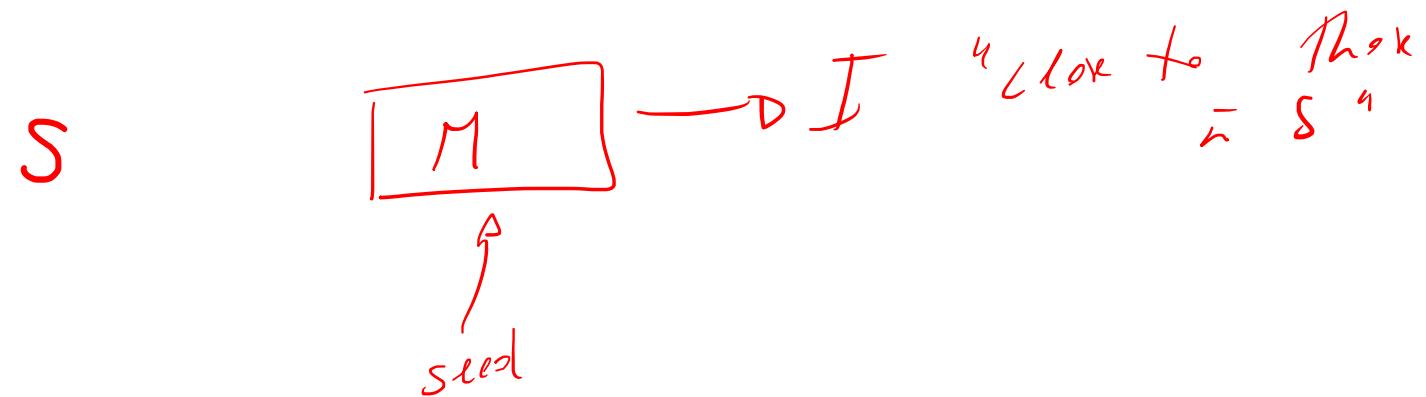
Autoencoders provide a **good initialization** (and reduce the risk of overfitting) because their latent vector is actually a **good (latent) representation** of the inputs used for training.



**Generative Models:  
Networks able to generate realistic images**

# Generative Models

Goal: generate, given a training set of images (data)  $S$ , other images (data) that are similar to those in  $S$



# What for generative models?

- Generative models can be used for **data augmentation**, simulation and planning
- Training generative models can also enable inference of latent representations that can be useful as general features
- Realistic samples for artwork, super-resolution, colorization, etc.
- You are getting close to the “holy grail” of modeling the distribution of natural images
  - This can be a very useful regularization prior in other problems or to perform anomaly detection

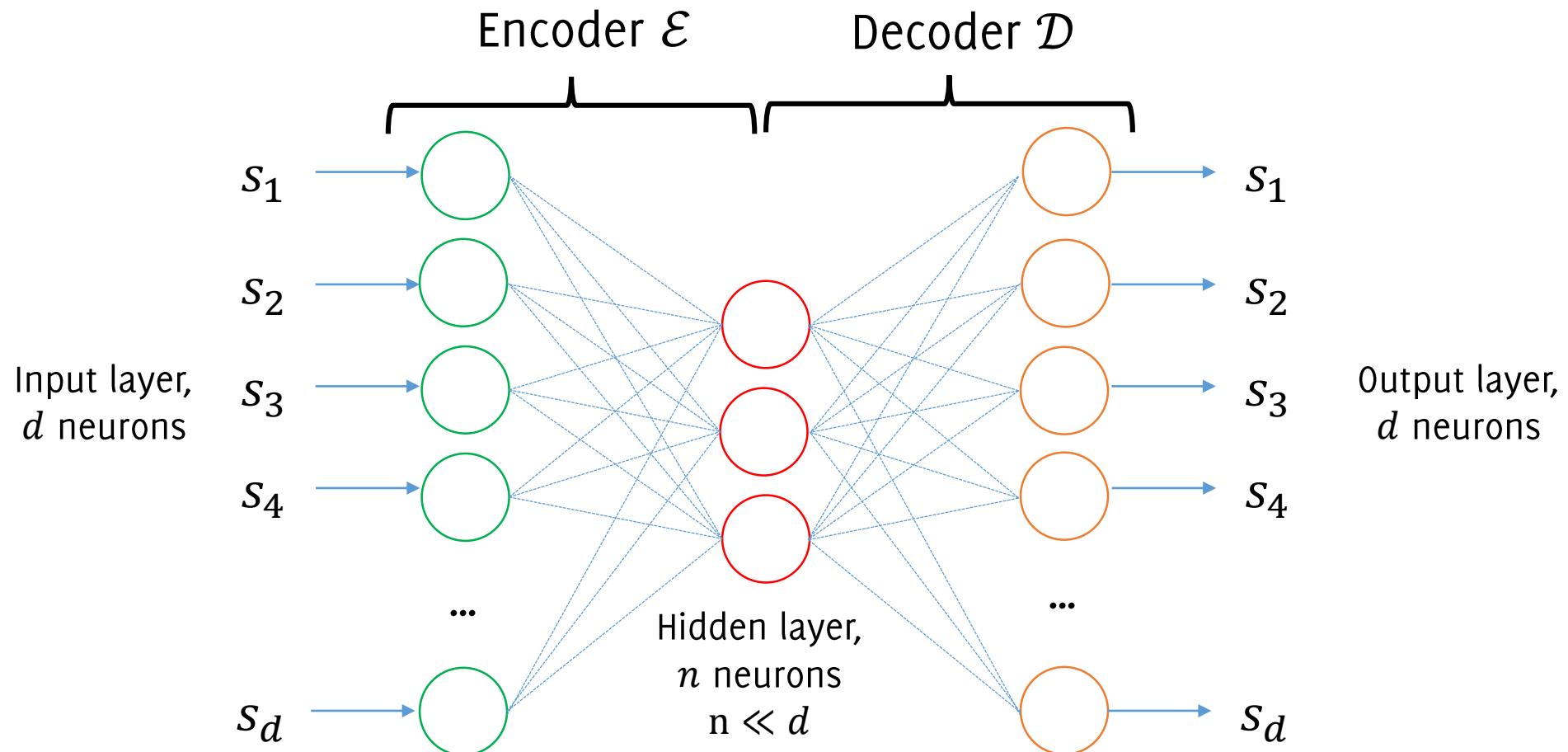
Images randomly generated by a GAN



# What about using Autoencoders as Generative Models?

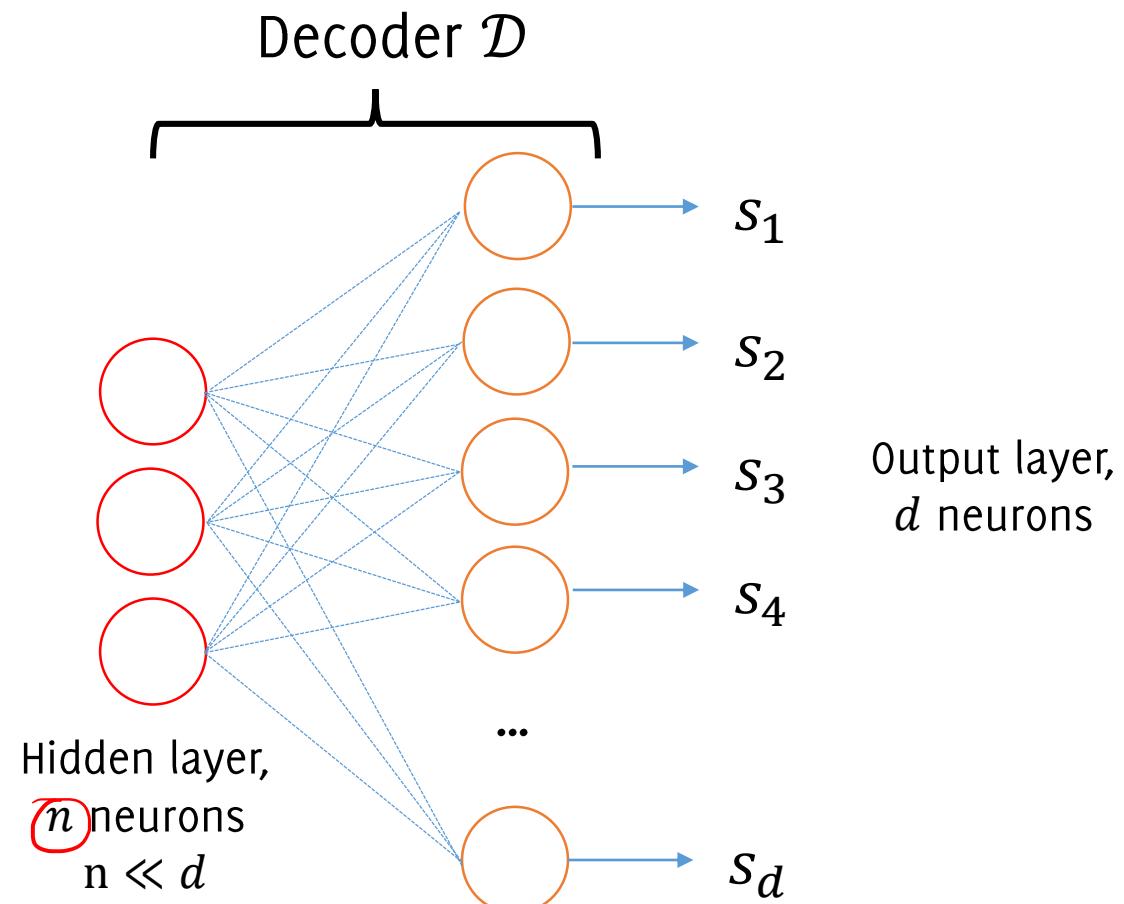
One option would be to

- 1) train an autoencoder on  $S$



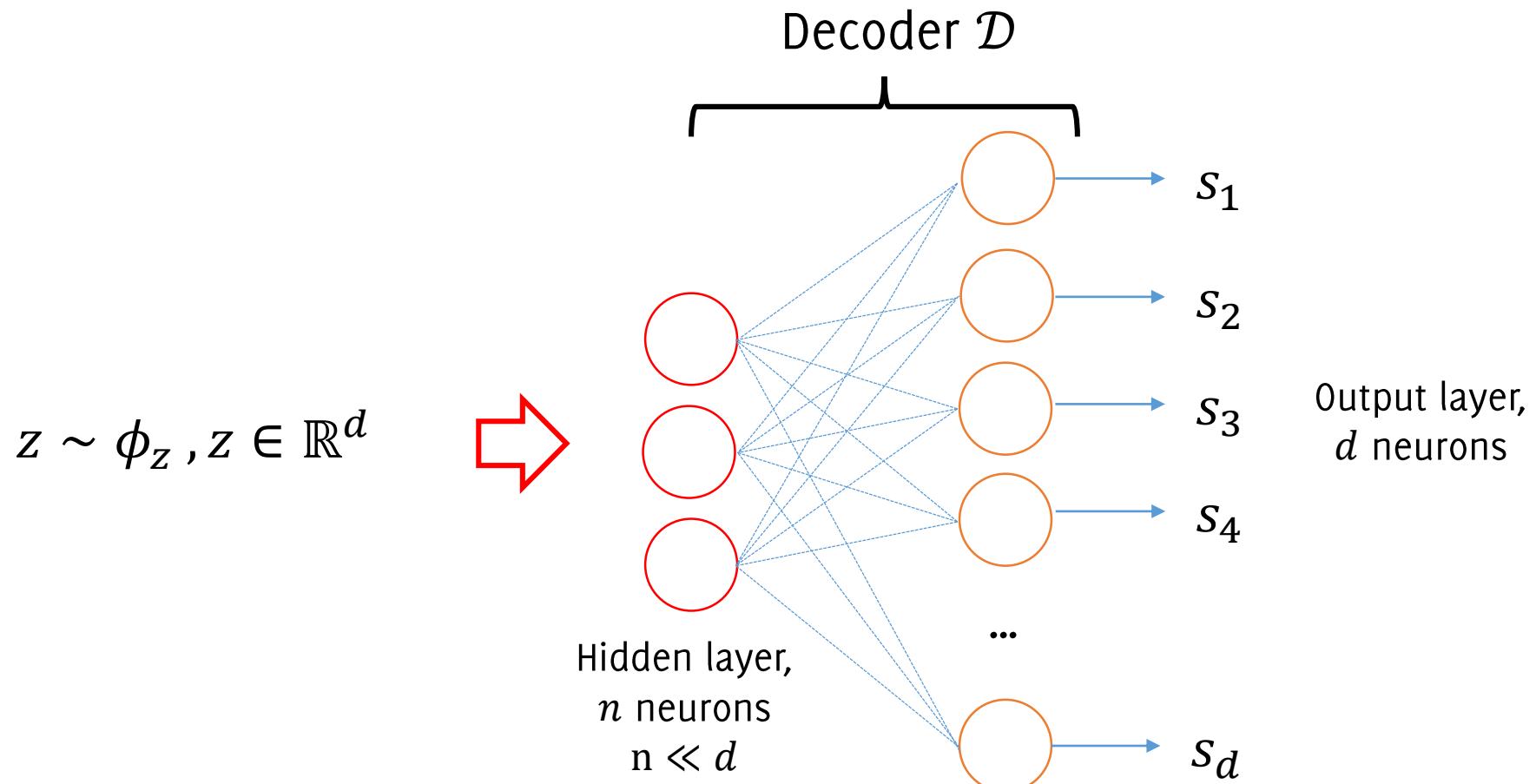
# What about using Autoencoders as Generative Models?

2) Discard the encoder



# What about using Autoencoders as Generative Models?

3) Draw random vectors  $z \sim \phi_z$ , to mimic «a new latent representation» and feed this to the decoder input

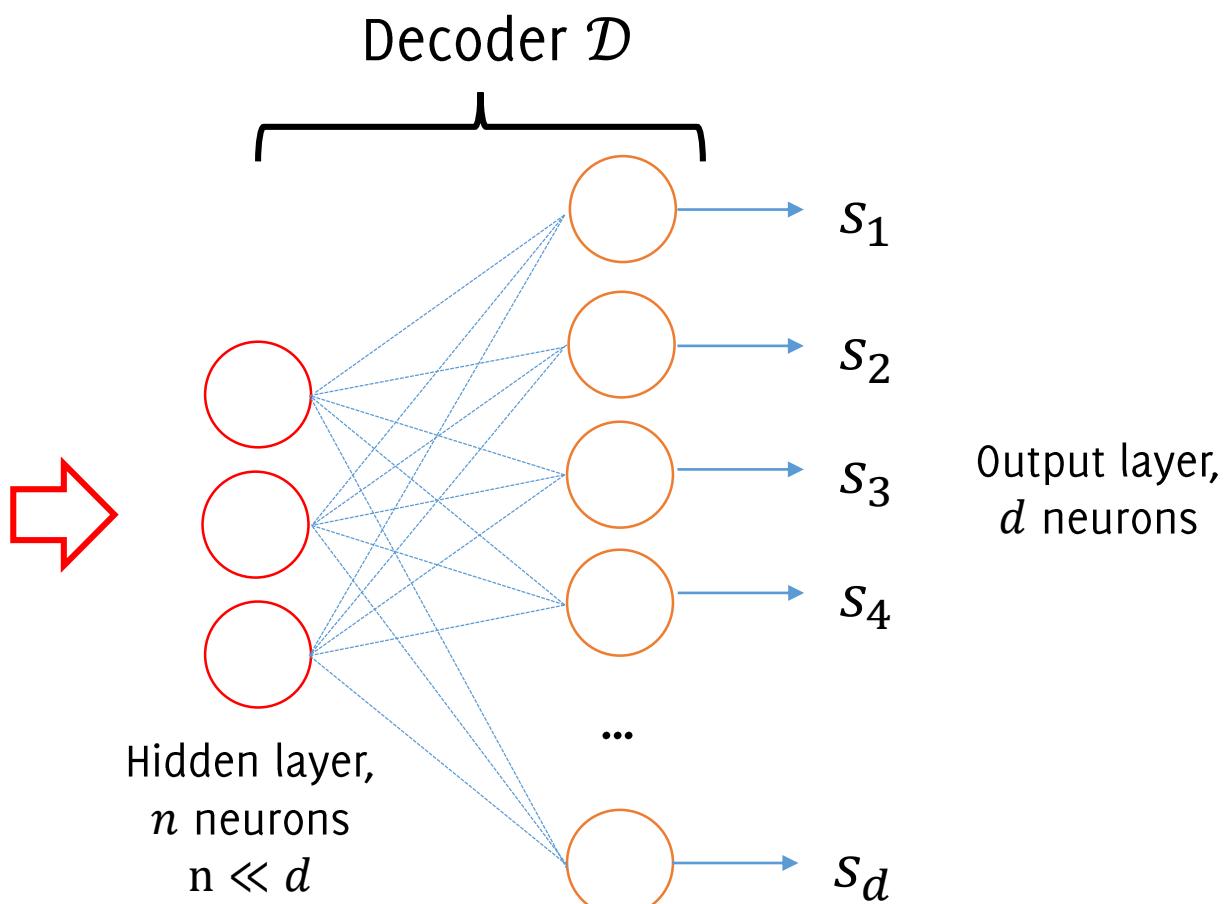


# What about using Autoencoders as Generative Models?

This approach does not work since **we do not know the distribution of proper latent representation** (or it is very difficult to estimate).

**Variational autoencoders**  
leverages a prior over  
z to generate images  
using a similar architecture

$$z \sim \phi_z, z \in \mathbb{R}^d$$



# **Generative Adversarial Networks**

A very effective way to generate images

# Generative Adversarial Networks (GAN)

## The GAN approach:

- Do not look for an explicit density model  $\phi_S$  describing the manifold of natural images.
- Just find out a model able to generate samples that «looks like» training samples  $S \subset \mathbb{R}^n$

Instead of sampling from  $\phi_S$ , just:

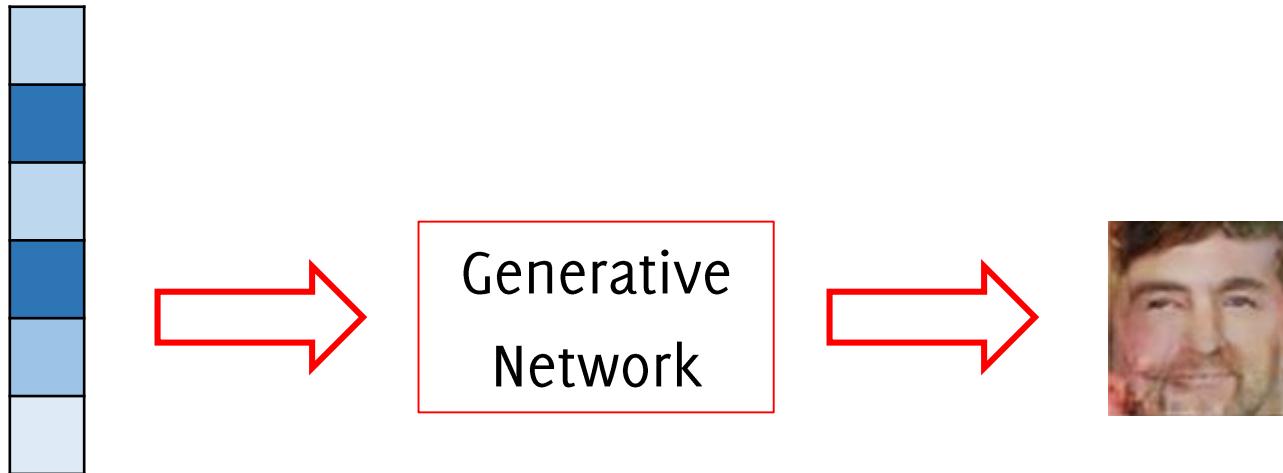
- **Sample a seed** from a known distribution  $\phi_z$ . This is defined a priori and also referred to as **noise**.
- Feed this seed to a learned transformation that generates realistic samples, as if they were drawn from  $\phi_S$

Use a neural network to learn this transformation

The neural network is going to be **trained in an unsupervised manner, no label needed**

# Generative Adversarial Networks (GAN)

The GAN approach:

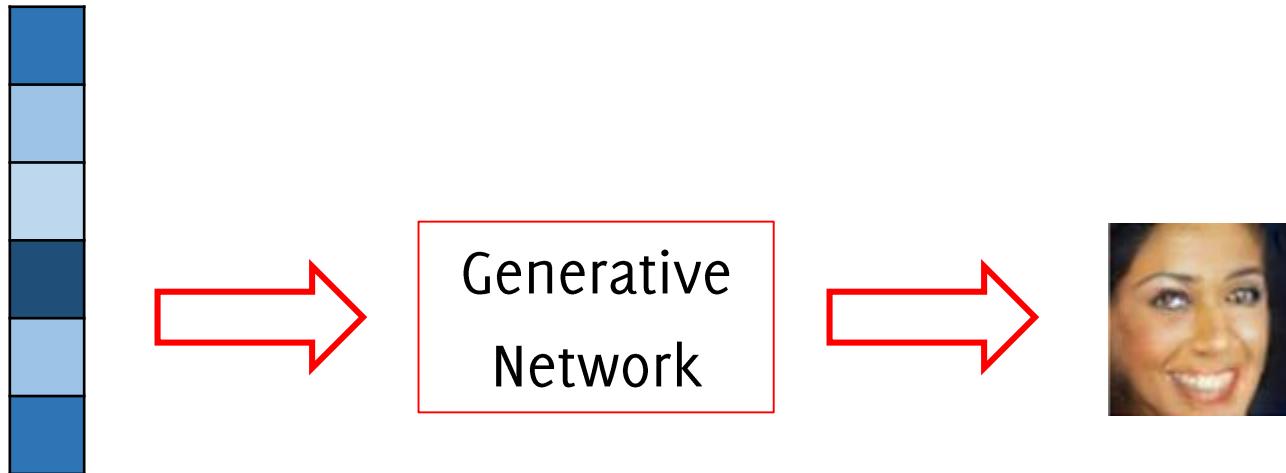


$$z \sim \phi_z$$

Draw a sample from  
the *noise distribution*

# Generative Adversarial Networks (GAN)

The GAN approach:



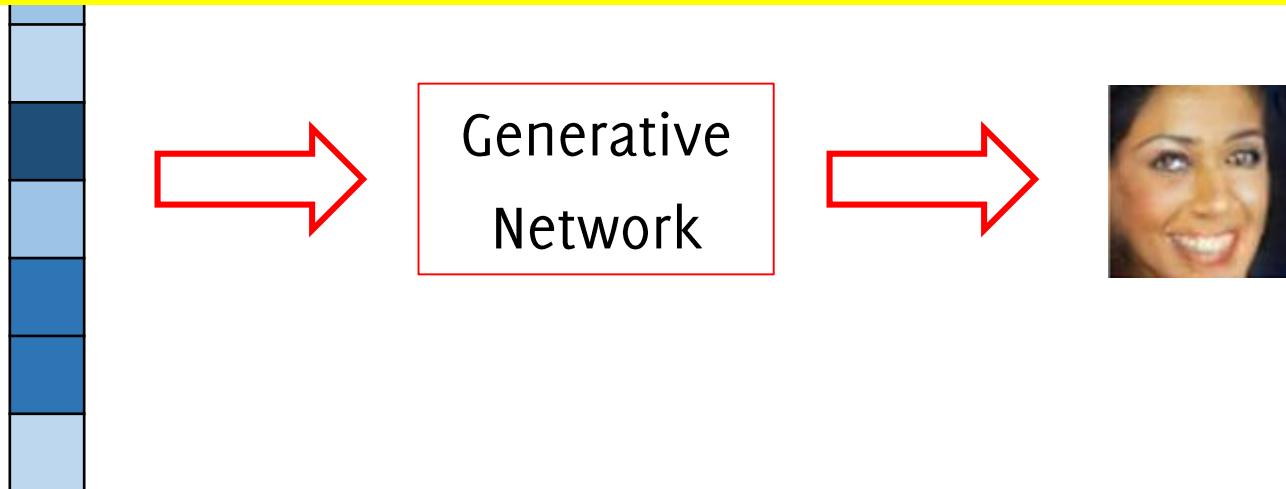
$$z \sim \phi_z$$

Draw a sample from  
the noise distribution

# Generative Adversarial Networks (GAN)

The GAN approach:

The biggest challenge is to define a suitable loss for assessing whether the output is a realistic image or not



$$z \sim \phi_z$$

Draw a sample from  
the noise distribution

# Generative Adversarial Networks (GAN)

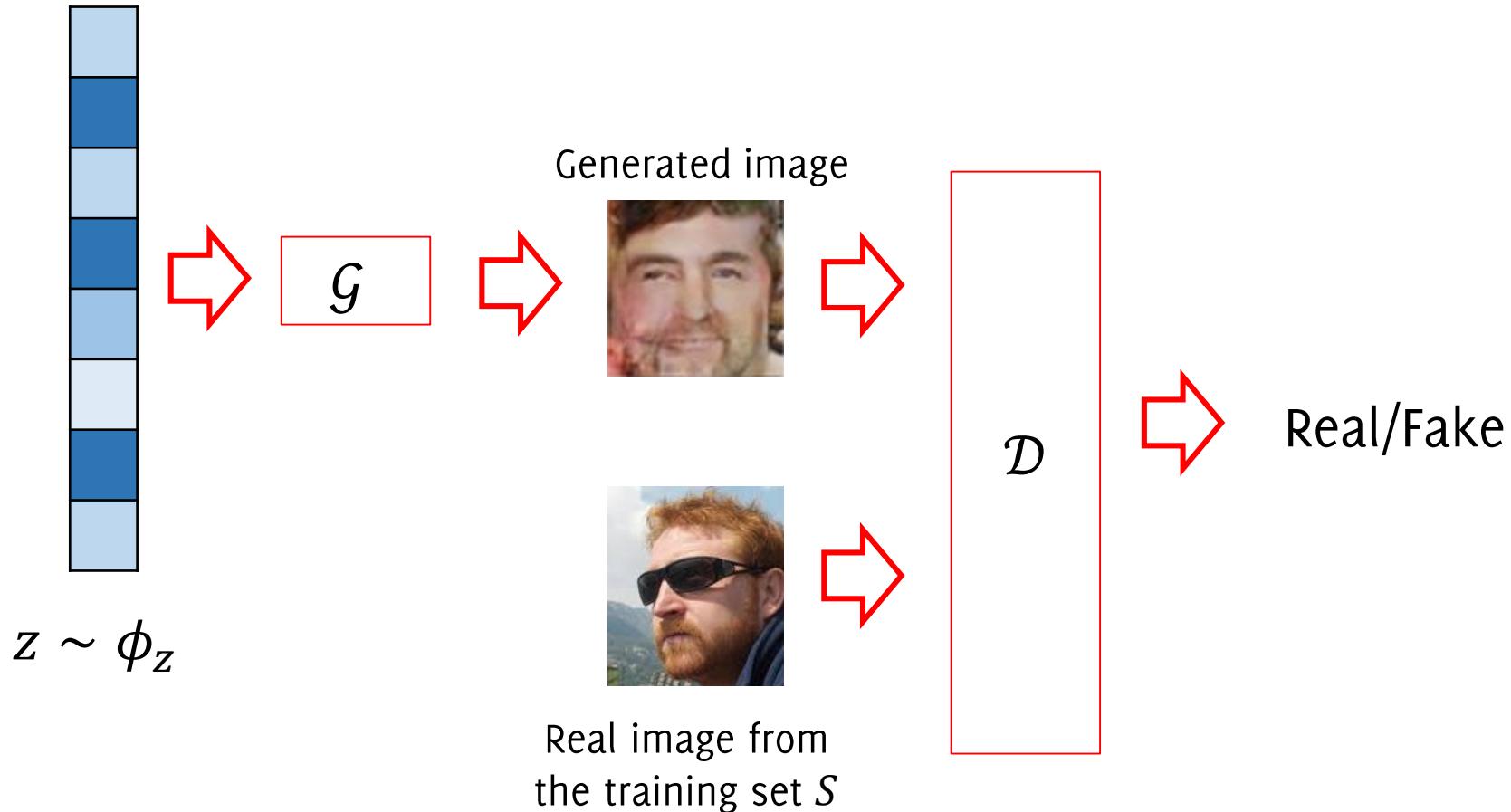
**The GAN solution:** Train a pair of neural networks addressing two different tasks that compete in a sort of two player (adversarial) game.

These models are:

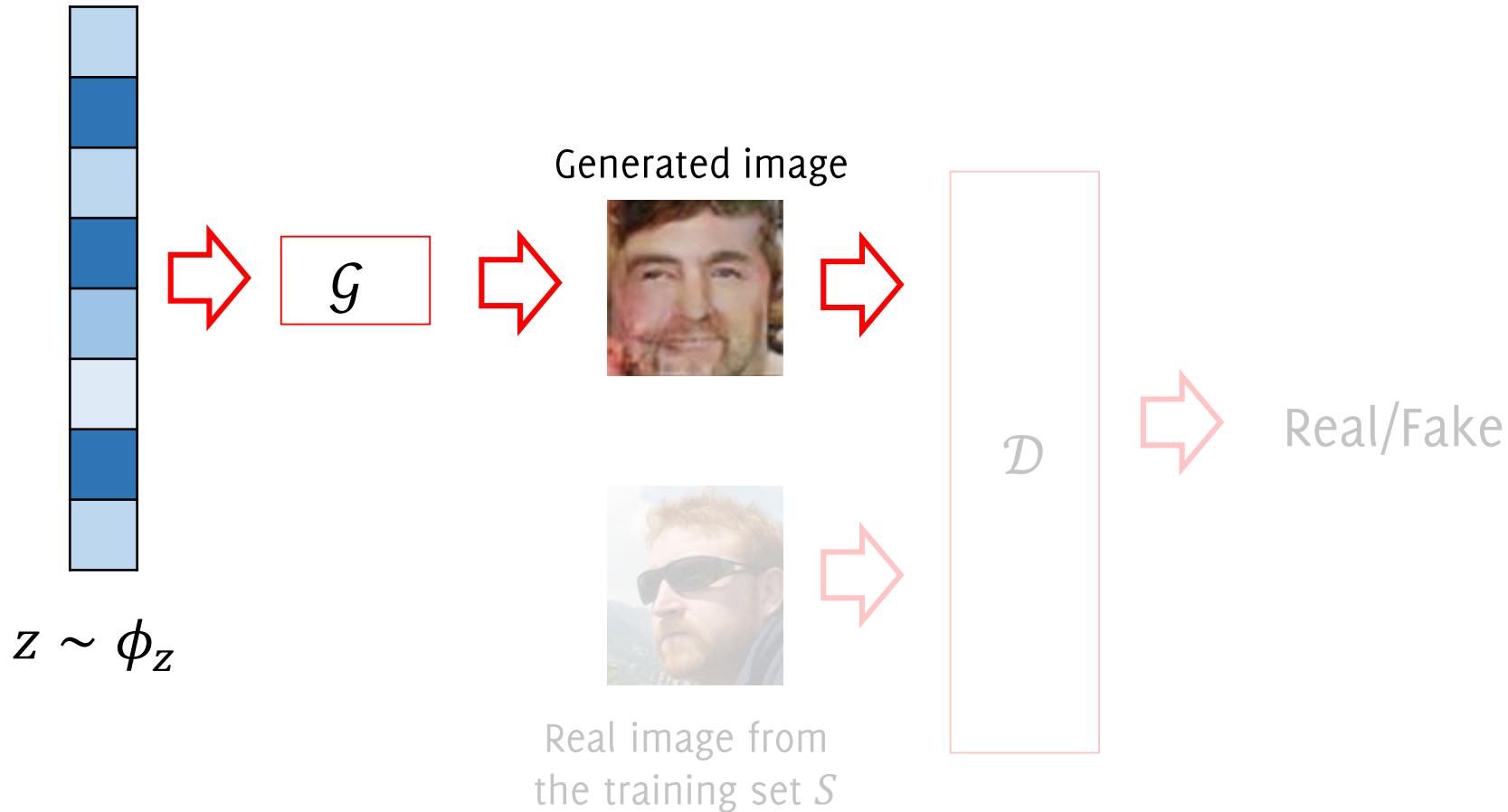
- **Generator  $\mathcal{G}$**  that produces realistic samples e.g. taking as input some random noise.  $\mathcal{G}$  tries to fool the discriminator
- **Discriminator  $\mathcal{D}$**  that takes as input an image and assess whether it is real or generated by  $\mathcal{G}$

Train the two and at the end, keep only  $\mathcal{G}$

# GAN Architecture



# Using GAN



Discriminator  $\mathcal{D}$  is completely useless and as such dropped. After a successful GAN training,  $\mathcal{D}$  is not able to distinguish the real/fake

# GAN: Setting up the stage

Both  $\mathcal{D}$  and  $\mathcal{G}$  are conveniently chosen as MLP or CNN

Our networks take as input:

- $\mathcal{D} = \mathcal{D}(s, \theta_d),$
- $\mathcal{G} = \mathcal{G}(z, \theta_g),$

$\theta_g$  and  $\theta_d$  are network parameters,  $s \in \mathbb{R}^n$  is an input image (either real or generated by  $\mathcal{G}$ ) and  $z \in \mathbb{R}^d$  is some random noise to be fed to the generator.

This notation is meant to visualize what are the NN parameters.. The network is taking a single input

Our networks give as output:

- $\mathcal{D}(\cdot, \theta_d): \mathbb{R}^n \rightarrow [0,1]$  gives as output the posterior for the input be a true image
- $\mathcal{G}(\cdot, \theta_d): \mathbb{R}^d \rightarrow \mathbb{R}^n$  gives as output the generated image

# GAN Training

A good discriminator is such:

- $\mathcal{D}(\mathbf{s}, \theta_d)$  is maximum when  $\mathbf{s} \in S$  (true image from the training set)
- $1 - \mathcal{D}(\mathbf{s}, \theta_d)$  is maximum when  $\mathbf{s}$  was generated from  $\mathcal{G}$
- $1 - \mathcal{D}(\mathcal{G}(\mathbf{z}, \theta_g), \theta_d)$  is maximum when  $\mathbf{z} \sim \phi_z$

Training  $\mathcal{D}$  consists in maximizing the **binary cross-entropy**

$$\max_{\theta_d} (\mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log(1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))])$$

Written using expectations

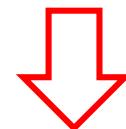
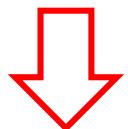
# GAN Training

A good discriminator is such:

- $\mathcal{D}(\mathbf{s}, \theta_d)$  is maximum when  $\mathbf{s} \in S$  (true image from the training set)
- $1 - \mathcal{D}(\mathbf{s}, \theta_d)$  is maximum when  $\mathbf{s}$  was generated from  $\mathcal{G}$
- $1 - \mathcal{D}(\mathcal{G}(\mathbf{z}, \theta_g), \theta_d)$  is maximum when  $\mathbf{z} \sim \phi_z$

Training  $\mathcal{D}$  consists in maximizing the binary cross-entropy

$$\max_{\theta_d} (\mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log(1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))])$$



This has to be 1  
since  $s \sim \phi_S$ , thus  
images are real

This has to be 0 since  
 $\mathcal{G}(\mathbf{z}, \theta_g)$  is a generated  
(fake) image

# GAN Training

A good discriminator is such:

- $\mathcal{D}(\mathbf{s}, \theta_d)$  is maximum when  $\mathbf{s} \in S$  (true image from the training set)
- $1 - \mathcal{D}(\mathbf{s}, \theta_d)$  is maximum when  $\mathbf{s}$  was generated from  $\mathcal{G}$
- $1 - \mathcal{D}(\mathcal{G}(\mathbf{z}, \theta_g), \theta_d)$  is maximum when  $\mathbf{z} \sim \phi_z$

Training  $\mathcal{D}$  consists in maximizing the binary cross-entropy

$$\max_{\theta_d} (\mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log(1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))])$$

A good generator  $\mathcal{G}$  makes  $\mathcal{D}$  to fail, thus minimizes the above

$$\min_{\theta_g} \max_{\theta_d} (\mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log(1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))])$$

# GAN Training

Solve by an iterative numerical approach

$$\min_{\theta_g} \max_{\theta_d} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log(1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

# GAN Training

Solve by an iterative numerical approach

$$\min_{\theta_g} \max_{\theta_d} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log (1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

**Alternate:**

- $k$ -steps of Stochastic Gradient Ascent w.r.t.  $\theta_d$ , keep  $\theta_g$  fixed and solve

$$\max_{\theta_d} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log (1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

- 1-step of Stochastic Grandient Descent w.r.t.  $\theta_g$  being  $\theta_d$  fixed

$$\min_{\theta_g} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log (1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

# GAN Training

for  $i = 1 \dots$  #number of epochs

for  $k$  –times # gradient ascent steps for  $\theta_d$

- Draw a minibatch  $\{\mathbf{z}_1, \dots, \mathbf{z}_m\}$  of noise realization
- Sample a minibatch of images  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\}$
- Update  $\theta_d$  by stochastic gradient ascend:

$$\nabla_{\theta_d} \left[ \sum_i \log \mathcal{D}(\mathbf{s}_i, \theta_d) + \log \left( 1 - \mathcal{D}(\mathcal{G}(\mathbf{z}_i, \theta_g), \theta_d) \right) \right]$$

Draw a minibatch  $\{\mathbf{z}_1, \dots, \mathbf{z}_m\}$  of noise realizations # gradient descent steps for  $\theta_g$

Update  $\mathcal{G}$  by stochastic gradient descent:

$$\nabla_{\theta_g} \left[ \sum_i \log \left( 1 - \mathcal{D}(\mathcal{G}(\mathbf{z}_i, \theta_g), \theta_d) \right) \right]$$

# GAN Training

```
for i = 1 ... #number of epochs
```

```
for k -times # gradient ascent steps for  $\theta_d$ 
```

- Draw a minibatch  $\{\mathbf{z}_1, \dots, \mathbf{z}_m\}$  of noise realization
- Sample a minibatch of images  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\}$
- Update  $\theta_d$  by stochastic gradient ascend:

$$\nabla_{\theta_d} \left[ \sum_i \log \mathcal{D}(\mathbf{s}_i, \theta_d) + \log \left( 1 - \mathcal{D}(\mathcal{G}(\mathbf{z}_i, \theta_g), \theta_d) \right) \right]$$

Draw a minibatch  $\{\mathbf{z}_1, \dots, \mathbf{z}_m\}$  of noise realizations # gradient descent steps for  $\theta_g$

Update  $\mathcal{G}$  by stochastic gradient descent:

$$\nabla_{\theta_g} \left[ \sum_i \log \left( 1 - \mathcal{D}(\mathcal{G}(\mathbf{z}_i, \theta_g), \theta_d) \right) \right]$$

This was presented as a best practice,  
latest GANs such as Wasserstein GANs do  
not use this

# One of the many GAN Training «trick»

1-step of Stochastic Gradient Descent w.r.t.  $\theta_g$  being  $\theta_d$  fixed

$$\min_{\theta_g} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} \left[ \log \left( 1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d) \right) \right] \right)$$

and since the first term does not depend on  $\theta_g$ , this consists in minimizing

$$\min_{\theta_g} \left( \mathbb{E}_{z \sim \phi_Z} \left[ \log \left( 1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d) \right) \right] \right)$$

or equivalently maximizing

$$\max_{\theta_g} \left( \mathbb{E}_{z \sim \phi_Z} \left[ \log \left( \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d) \right) \right] \right)$$

## GAN Training

Maximizing w.r.t  $\theta_g$  (instead of minimizing as before) does not modify the global solution of the min-max problem, but provides a stronger gradient during the early learning stages

Solve by an iterative numerical approach

$$\min_{\theta_g} \max_{\theta_d} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log (1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

Alternate:

- $k$ -steps of Stochastic Gradient Ascent w.r.t.  $\theta_d$  to solve

$$\max_{\theta_d} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log (1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

- 1-step of Stochastic Gradient Ascent w.r.t.  $\theta_g$  being  $\theta_d$  fixed

$$\min_{\theta_g} \left( \mathbb{E}_{s \sim \phi_S} [\log \mathcal{D}(s, \theta_d)] + \mathbb{E}_{z \sim \phi_Z} [\log (1 - \mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

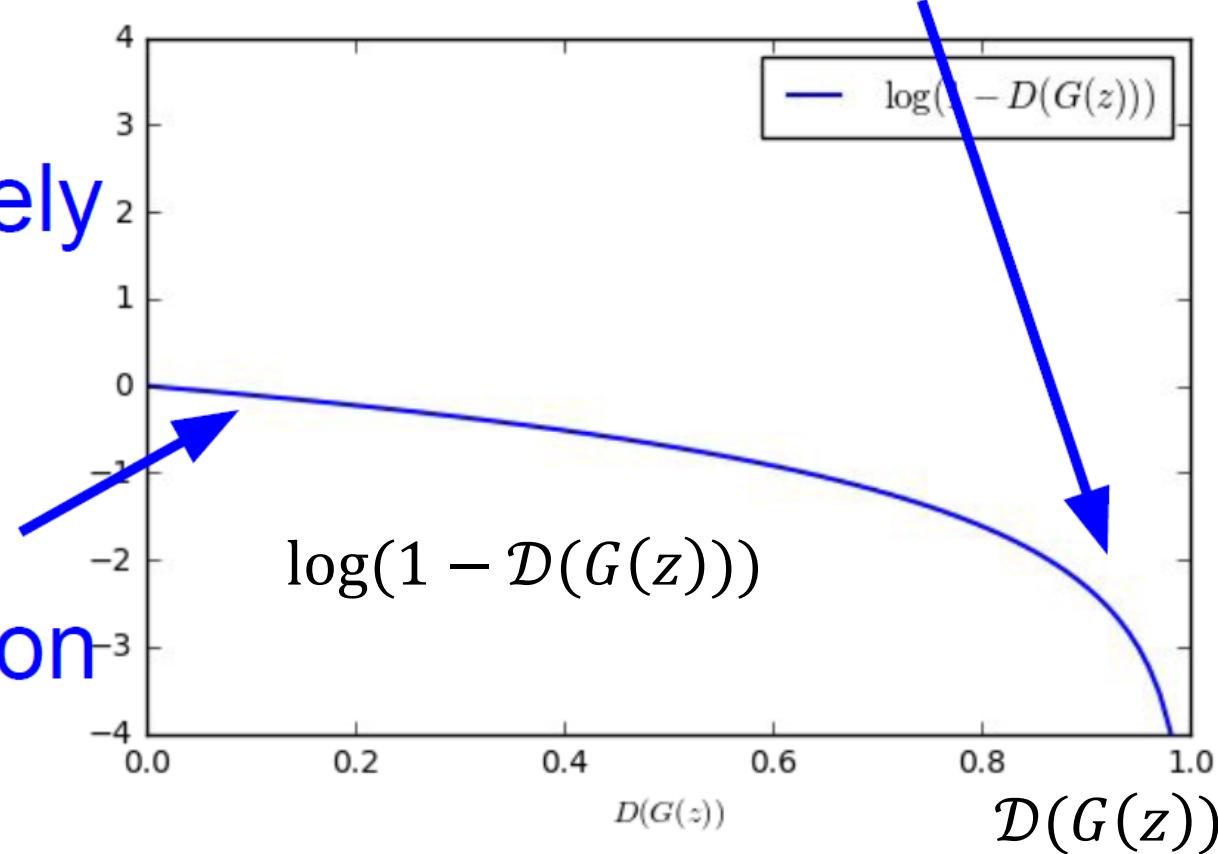
and since the first term does not depend on  $\theta_g$ , this consists in maximizing

$$\max_{\theta_g} \left( \mathbb{E}_{z \sim \phi_Z} [\log (\mathcal{D}(\mathcal{G}(z, \theta_g), \theta_d))] \right)$$

*During early learning stages, when  $G$  is poor,  $D$  can reject samples with high confidence because they are clearly different from the training data (thus  $D(G(z)) \approx 0$ ). In this case,  $\log(1 - D(G(z)))$  is flat, thus has very low gradient.*

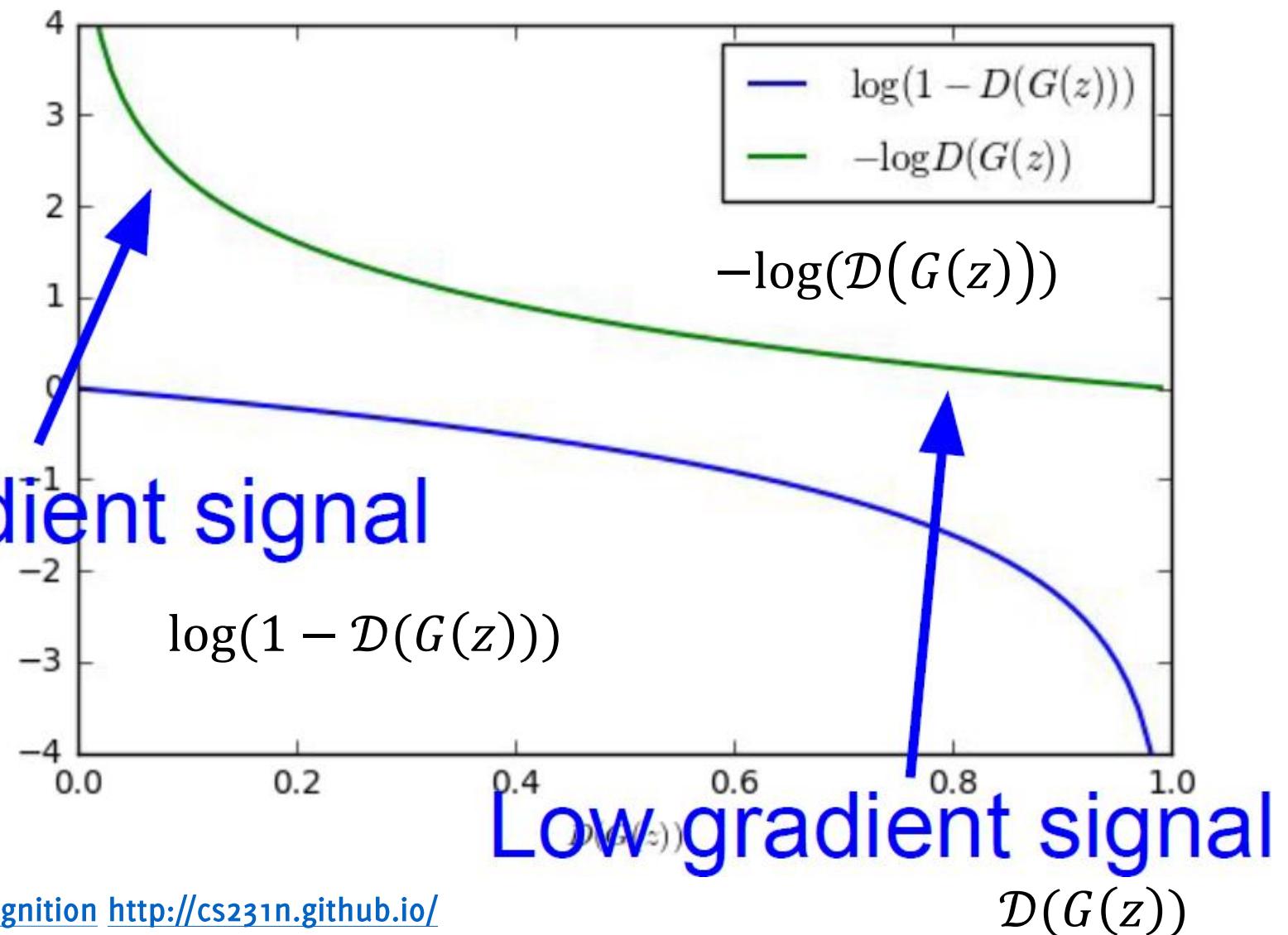
**When sample is likely fake, want to learn from it to improve generator. But gradient in this region is relatively flat!**

Gradient signal dominated by region where sample is already good



Rather than training  $G$  to minimize  $\log(1 - D(G(z)))$  we can train  $G$  to maximize  $\log(D(G(z)))$  [or as in this figure, minimize  $-\log(D(G(z)))$ ] This objective function results in the same fixed point of the dynamics of  $G$  and  $D$ , but provides much stronger gradients early in learning.

High gradient signal



# Algorithm outline

---

**Algorithm 1** Minibatch stochastic gradient descent training of generative adversarial nets. The number of steps to apply to the discriminator,  $k$ , is a hyperparameter. We used  $k = 1$ , the least expensive option, in our experiments.

---

**for** number of training iterations **do**

**for**  $k$  steps **do**

- Sample minibatch of  $m$  noise samples  $\{\mathbf{z}^{(1)}, \dots, \mathbf{z}^{(m)}\}$  from noise prior  $p_g(\mathbf{z})$ .
- Sample minibatch of  $m$  examples  $\{\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)}\}$  from data generating distribution  $p_{\text{data}}(\mathbf{x})$ .
- Update the discriminator by ascending its stochastic gradient:

$$\nabla_{\theta_d} \frac{1}{m} \sum_{i=1}^m \left[ \log D \left( \mathbf{x}^{(i)} \right) + \log \left( 1 - D \left( G \left( \mathbf{z}^{(i)} \right) \right) \right) \right].$$

**end for**

- Sample minibatch of  $m$  noise samples  $\{\mathbf{z}^{(1)}, \dots, \mathbf{z}^{(m)}\}$  from noise prior  $p_g(\mathbf{z})$ .

- Update the generator by descending its stochastic gradient:

$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log \left( 1 - D \left( G \left( \mathbf{z}^{(i)} \right) \right) \right).$$

**end for**

The gradient-based updates can use any standard gradient-based learning rule. We used momentum in our experiments.

# GAN Training

for  $i = 1 \dots$  #number of epochs

for  $k$  –times # gradient ascent steps for  $\theta_d$

- Draw a minibatch  $\{\mathbf{z}_1, \dots, \mathbf{z}_m\}$  of noise realization
- Sample a minibatch of images  $\{\mathbf{s}_1, \dots, \mathbf{s}_m\}$
- Update  $\theta_d$  by stochastic gradient ascend:

$$\nabla_{\theta_d} \left[ \sum_i \log \mathcal{D}(\mathbf{s}_i, \theta_d) + \log(1 - \mathcal{D}(\mathcal{G}(\mathbf{z}_i, \theta_g), \theta_d)) \right]$$

Draw a minibatch  $\{\mathbf{z}_1, \dots, \mathbf{z}_m\}$  of noise realizations # gradient descent steps for  $\theta_g$

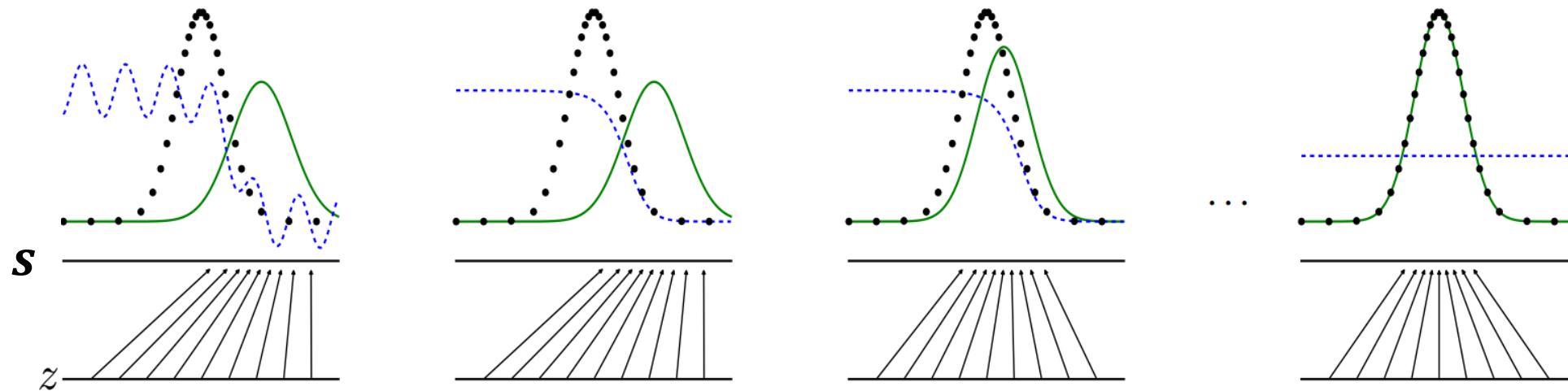
Update  $\mathcal{G}$  by stochastic gradient **ascent**:

$$\nabla_{\theta_g} \left[ \sum_i \log(\mathcal{D}(\mathcal{G}(\mathbf{z}_i, \theta_g), \theta_d)) \right]$$

# Illustration of the GAN Training Process

In this illustration  $\mathbb{R}^d$  and  $\mathbb{R}^n$  are collapsed into 1d points  
this allows also the visualization of their distribution

.....  $\phi_s$ ,  $s$  real  
—  $\phi_{G(z)}$   $G(z)$  fake  
- - -  $D(\cdot)$   $D$  posterior



# At the end of the day...

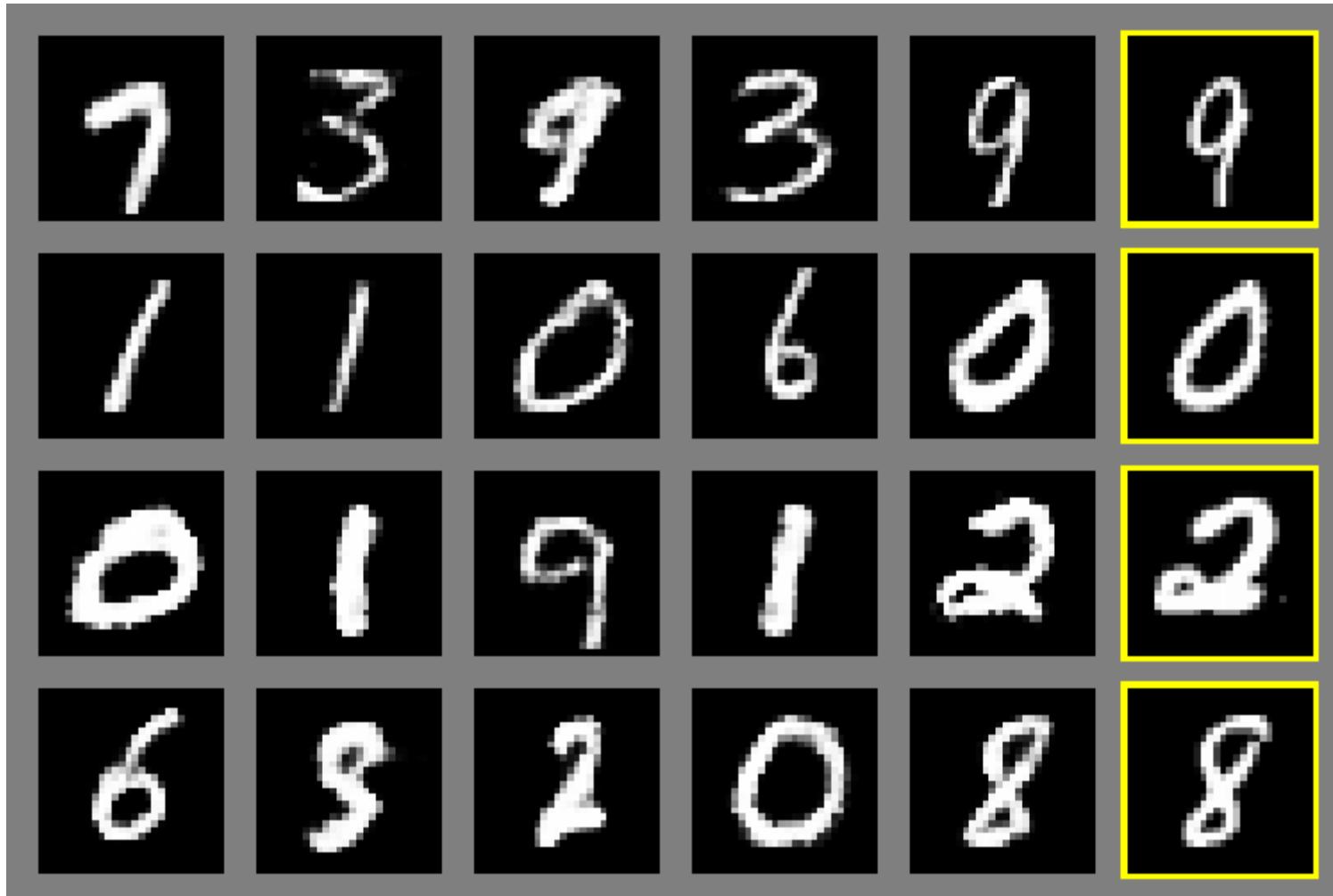
The discriminator  $\mathcal{D}$  is discarded

The generator  $\mathcal{G}$  and  $\phi_z$  are preserved as generative model

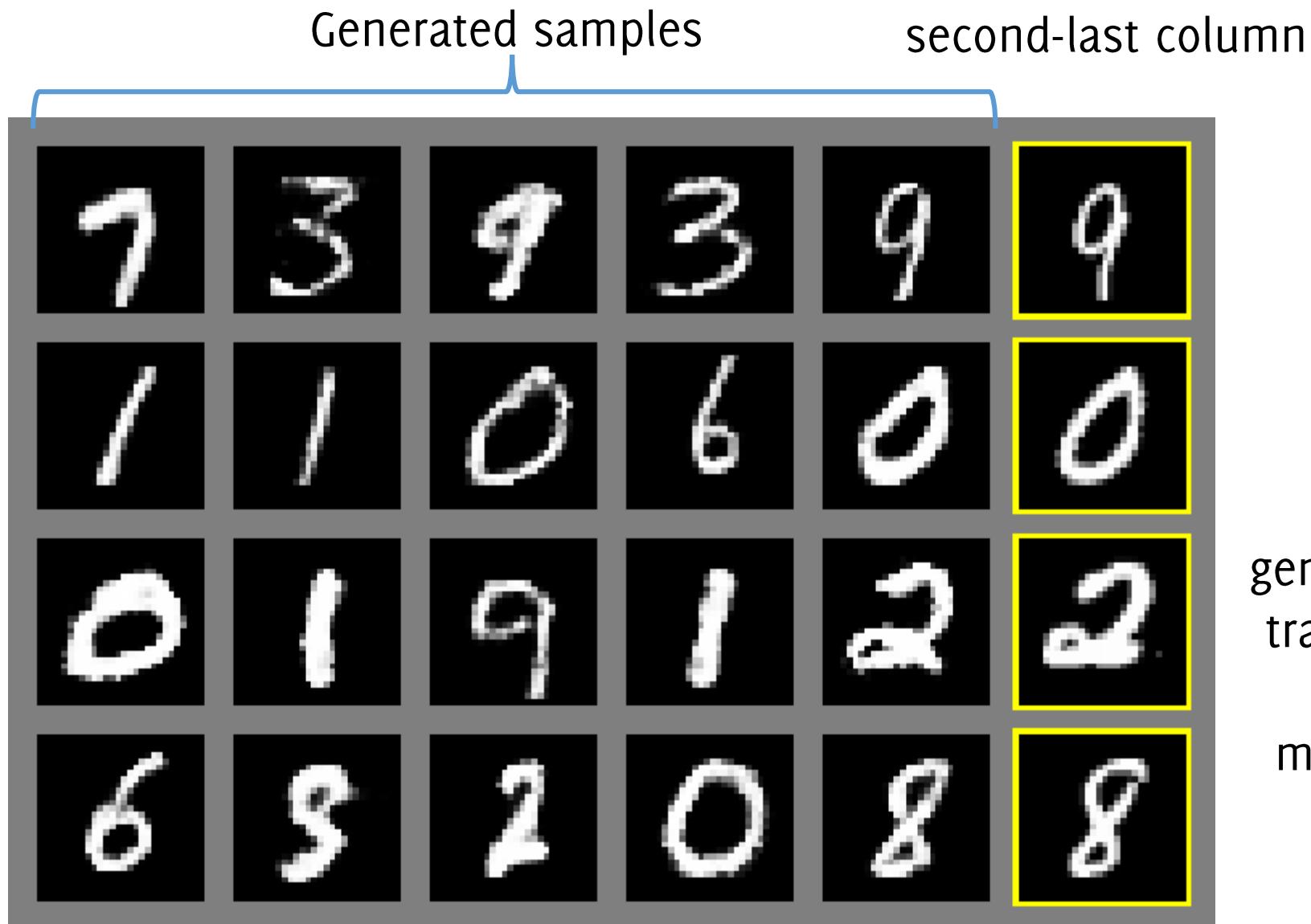
Remarks:

- **The training is rather unstable**, need to carefully synchronize the two steps (many later works in this direction, e.g. Wasserstein GAN)
- **Training by standard tools**: backpropagation and dropout
- Theoretical results provided
- **Generator does not use  $S$  directly during training**
- **Generator performance is difficult to assess quantitatively**
- There is **no explicit expression for the generator**, it is provided in an implicit form -> you cannot compute the likelihood of a sample w.r.t. the learned GAN

# MNIST



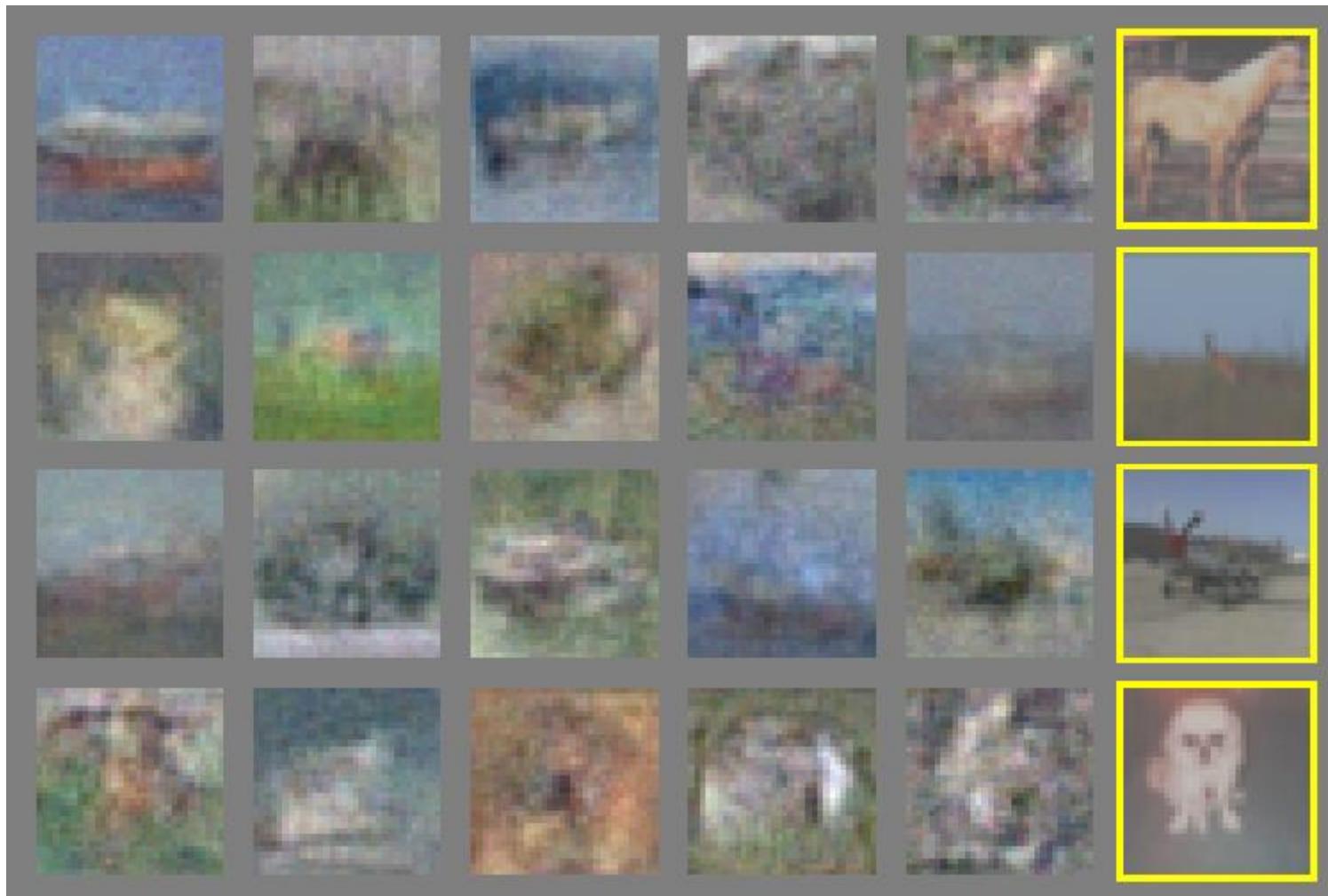
# MNIST



# Toronto Face Database (TFD)



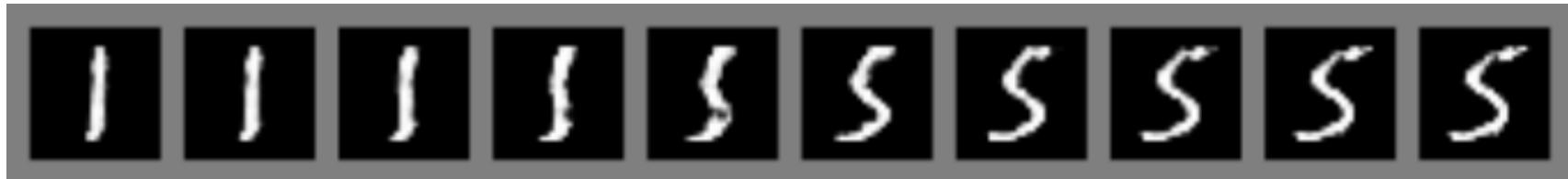
# CIFAR-10



# Outputs of interpolated trajectories

Select two noise realization  $z_1$  and  $z_2$  yielding reasonable outputs, and interpolate among the two. Generate the images of intermediate values

$\mathcal{G}(z_1)$

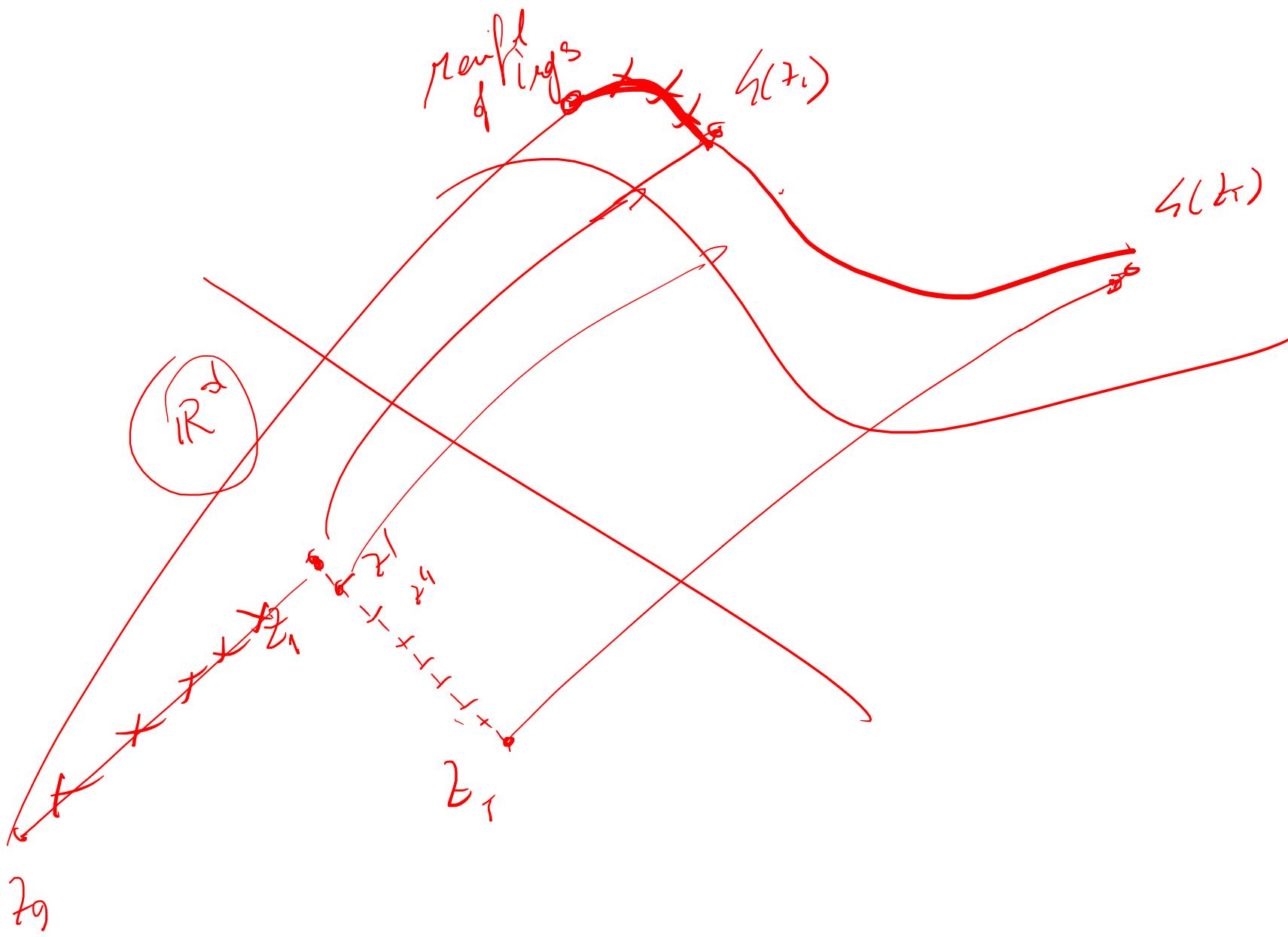


$\mathcal{G}(z_2)$

$\mathcal{G}(z_3)$



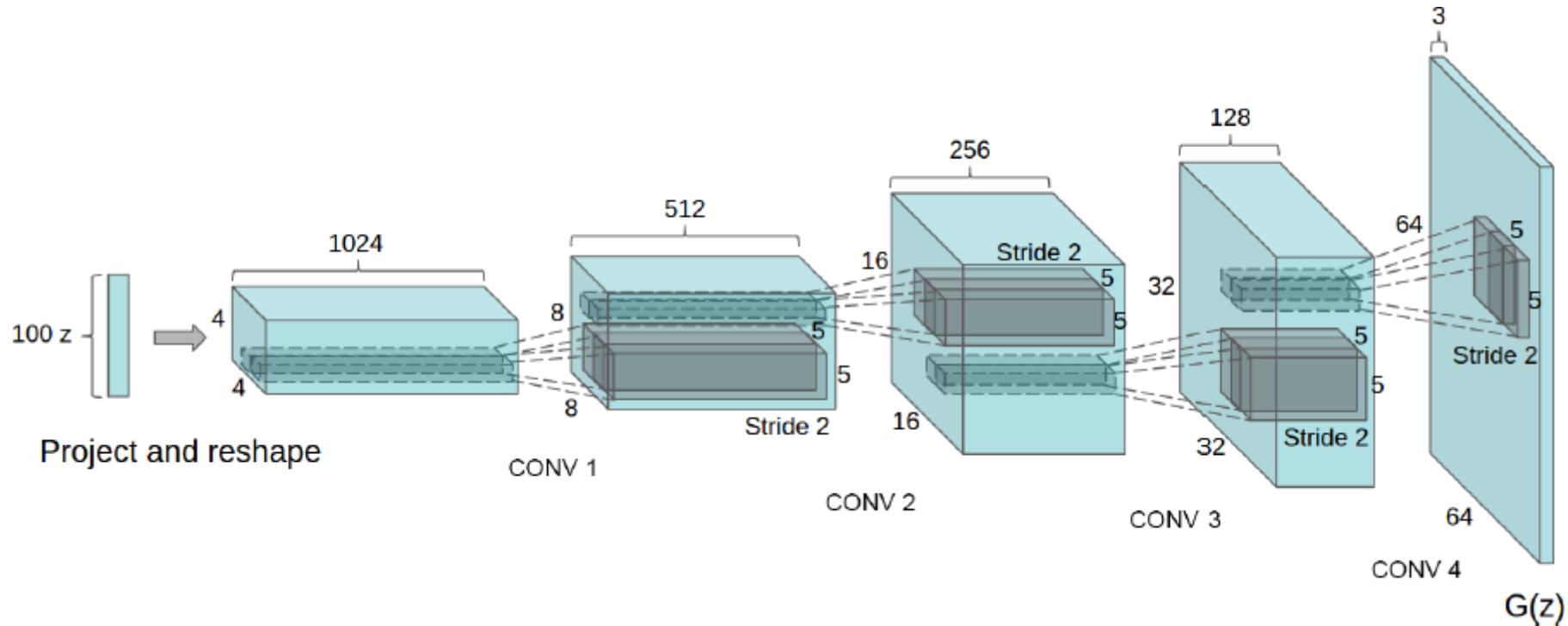
$\mathcal{G}(z_4)$



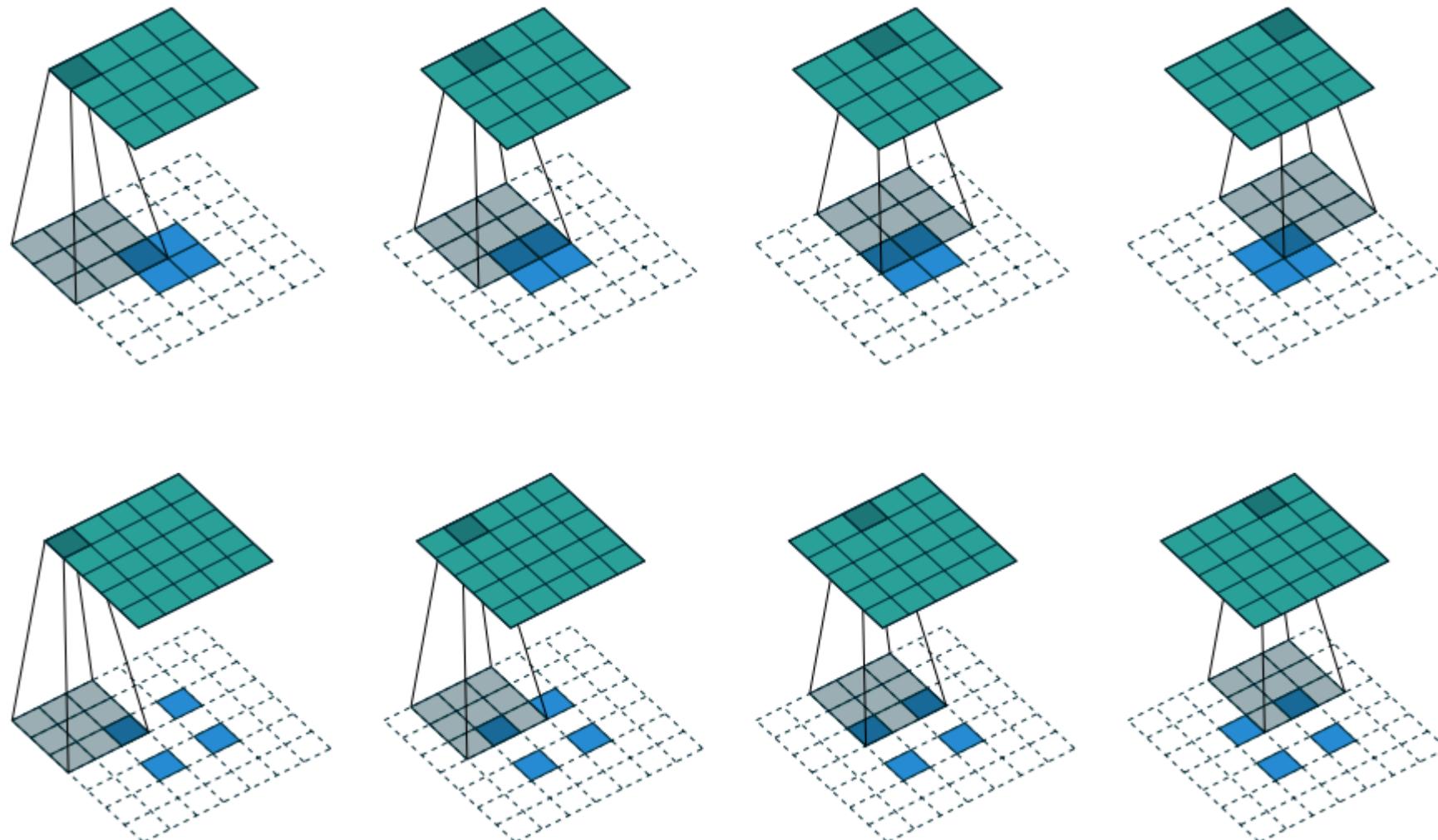
# GANs have much improved in the last few years

DC-GAN: Deep Convolutional GANs

RGB Image



# How is it possible to "increase the network" size?



# GANs have much improved in the last few years

Images generated after 1 training epochs

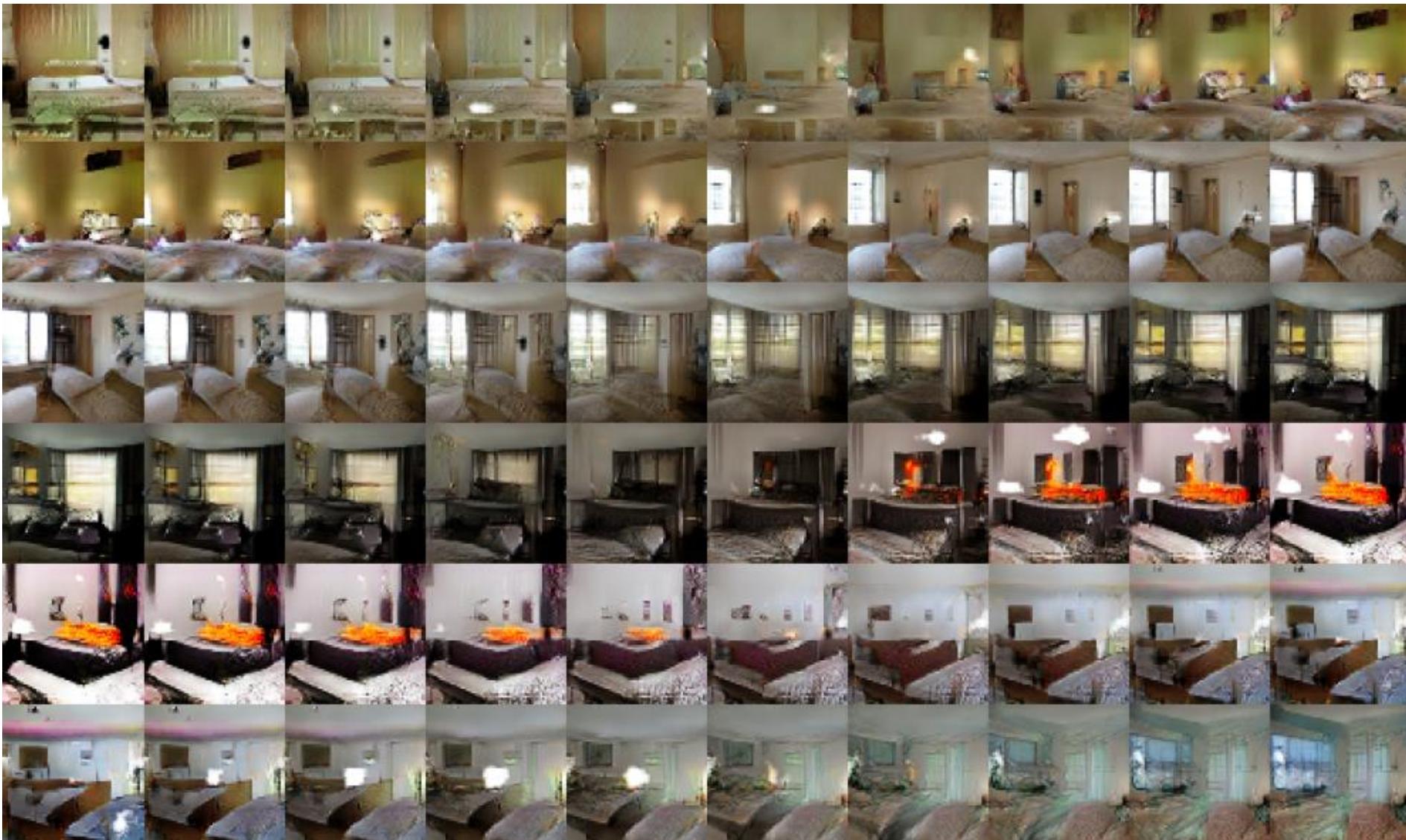


# GANs have much improved in the last few years

Images generated after 5 training epochs



# Interpolation between a series of 9 random points



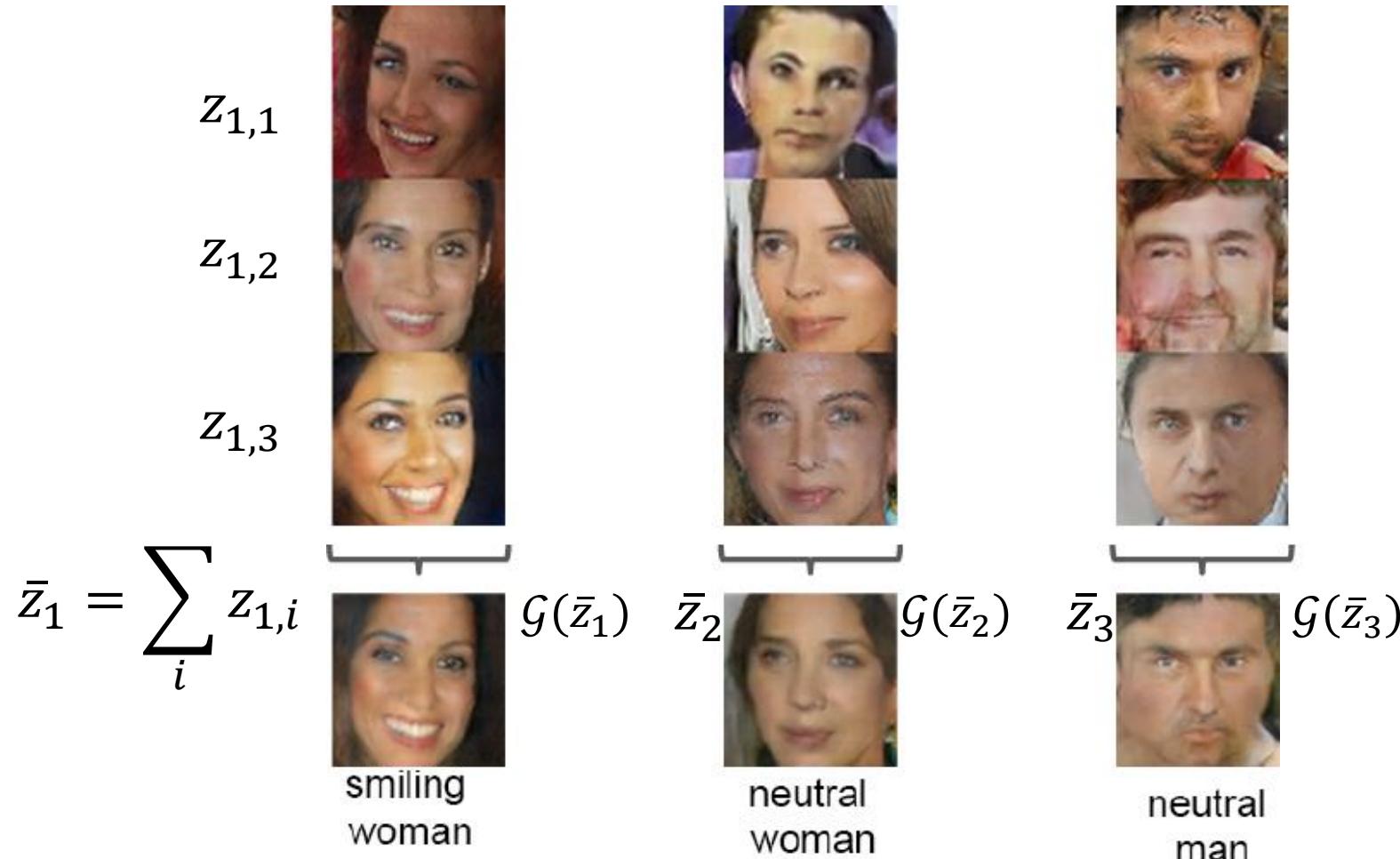
# Vector Arithmetic



Take randomly generated samples of smiling women, neutral women, and neutral men

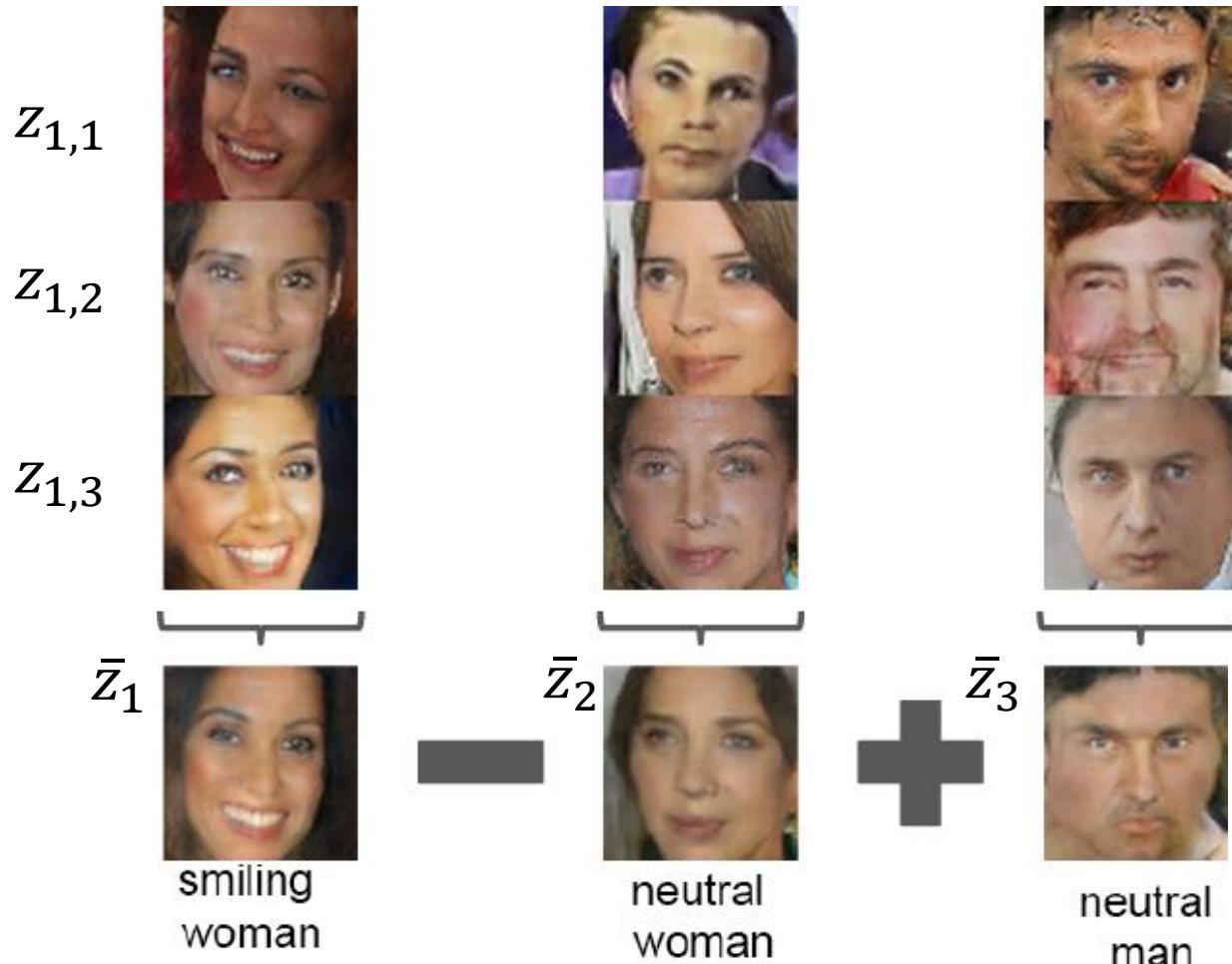
# Vector Arithmetic

Average the corresponding noise seeds



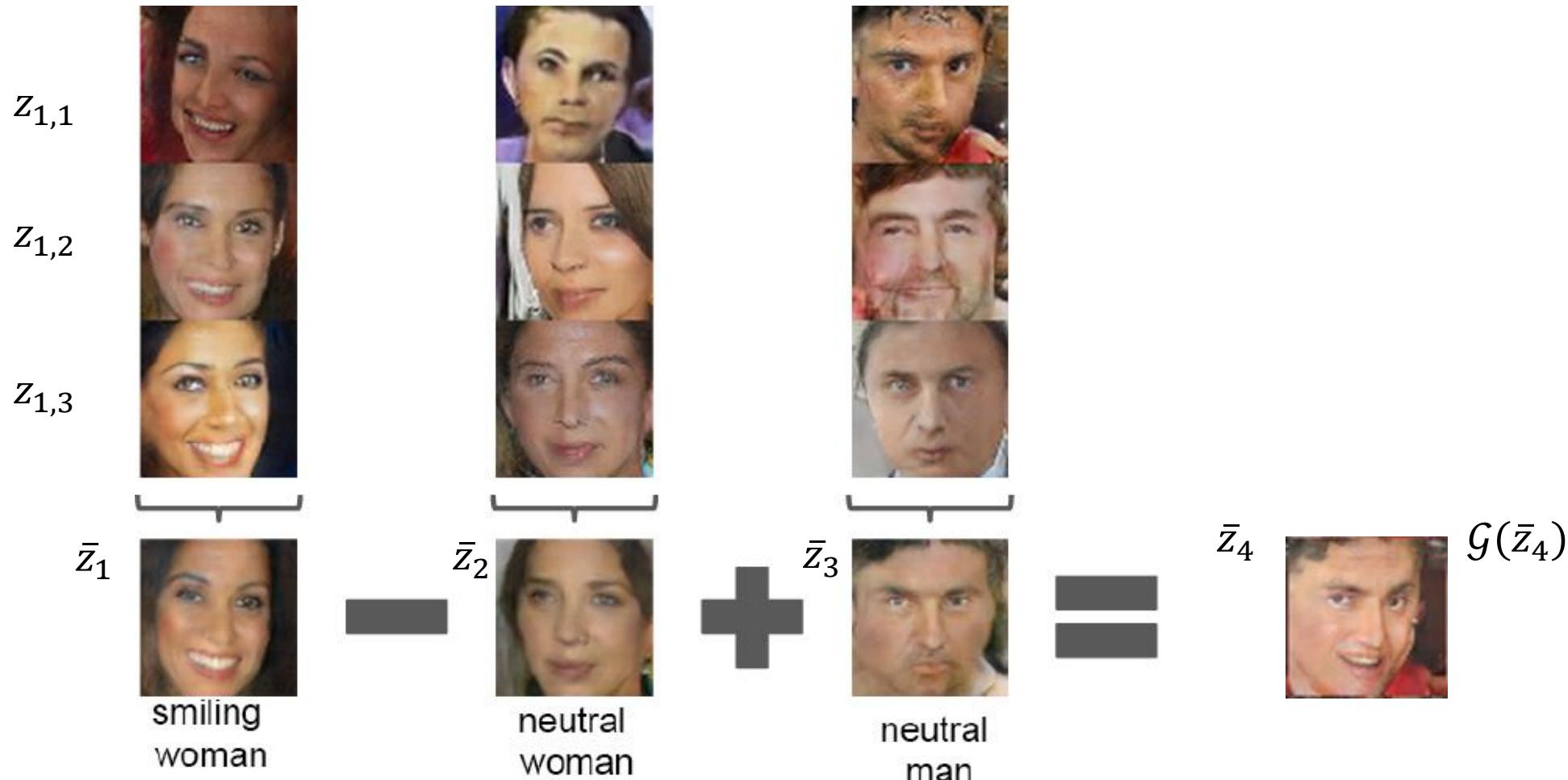
# Vector Arithmetic

Perform some arithmetic



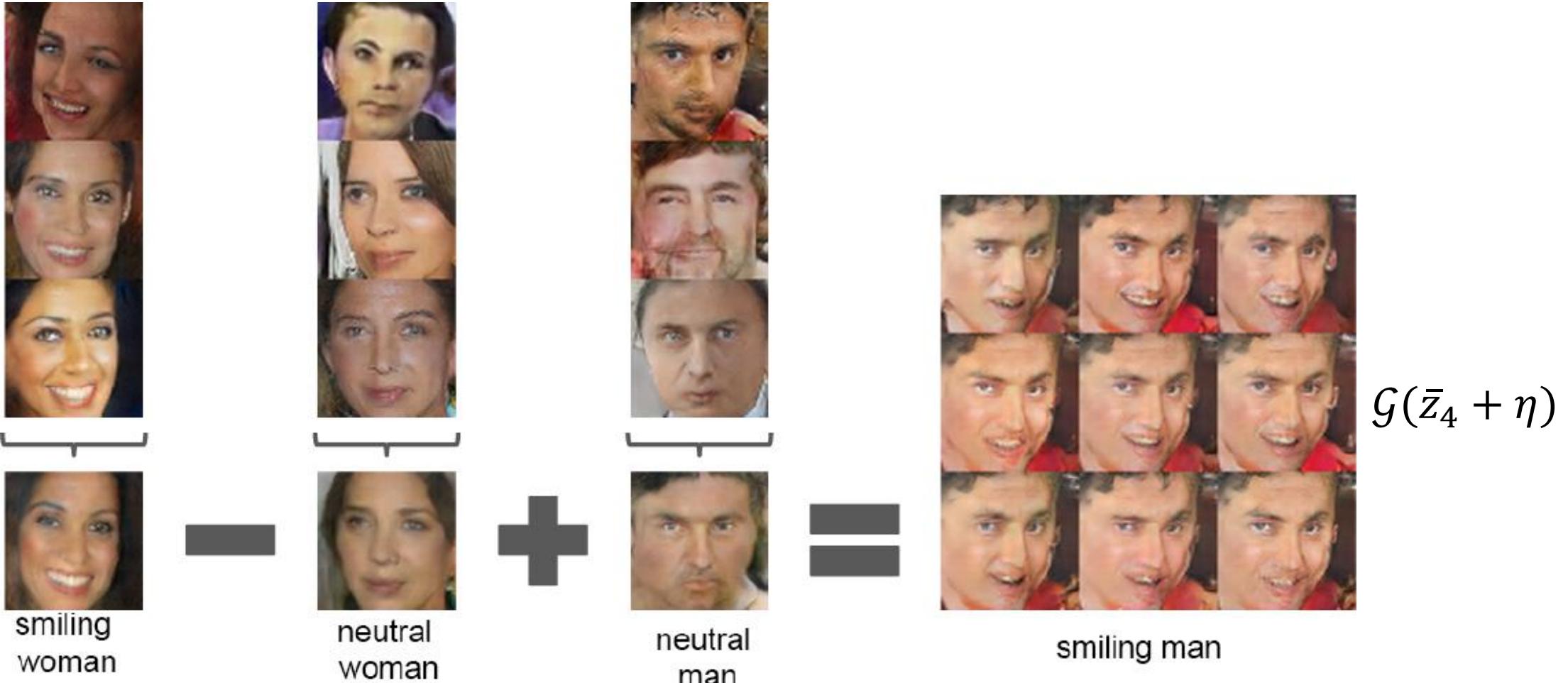
# Vector Arithmetic

Perform some arithmetic  $\bar{z}_1 - \bar{z}_2 + \bar{z}_3 = \bar{z}_4$



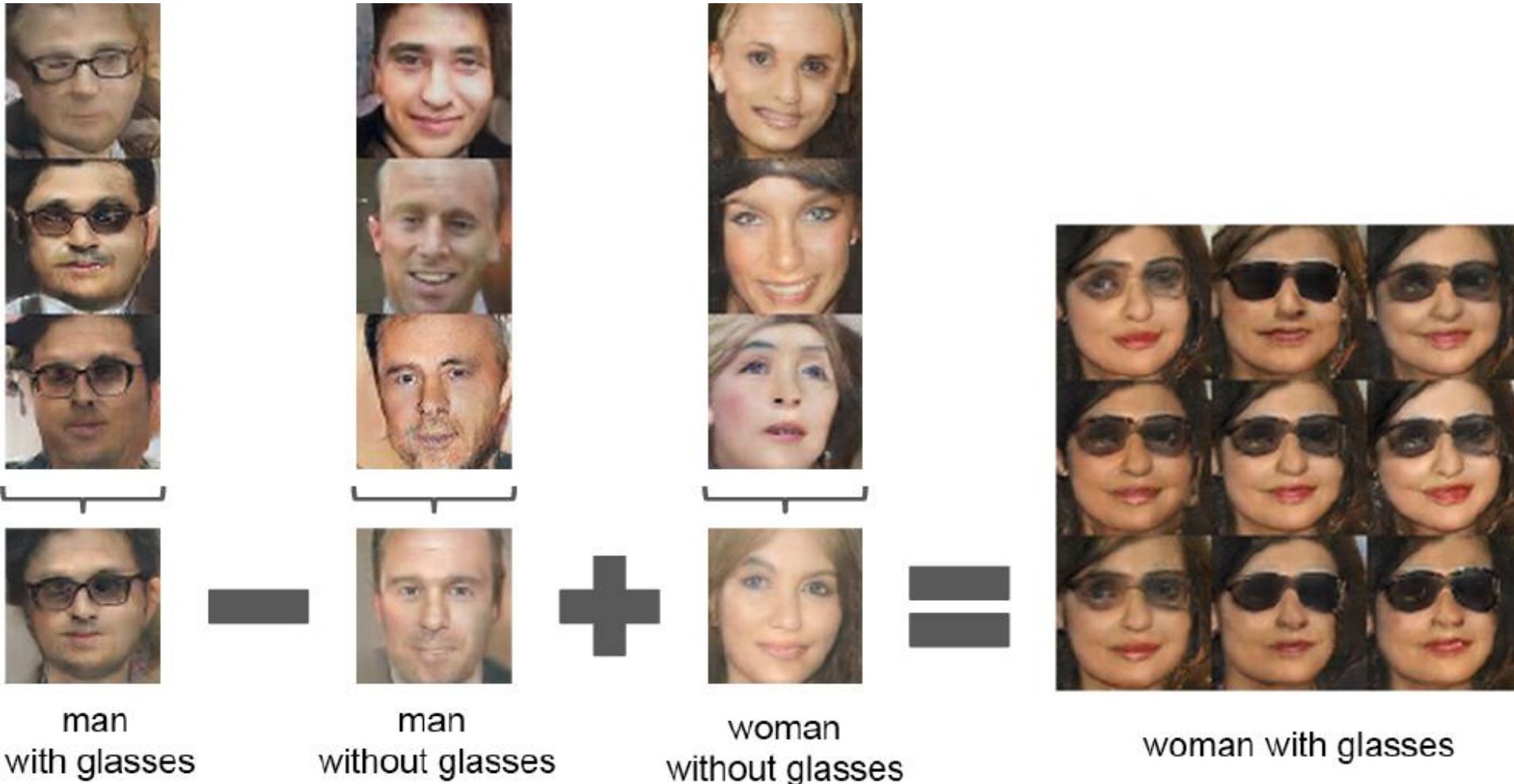
# Vector Arithmetic

Add some noise to the input vector and that's pretty robust



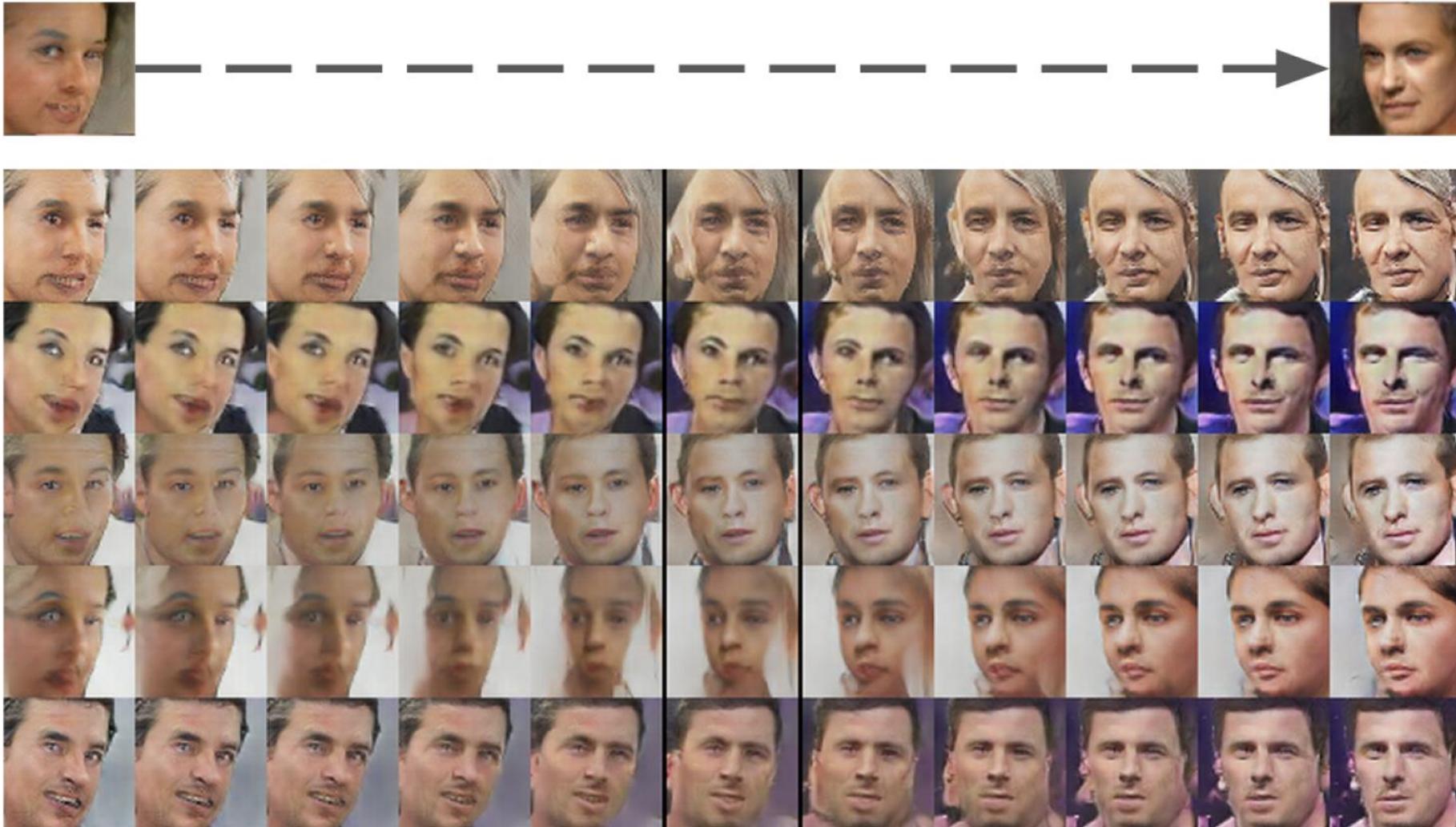
# Vector Arithmetic

Similar example as word embedding

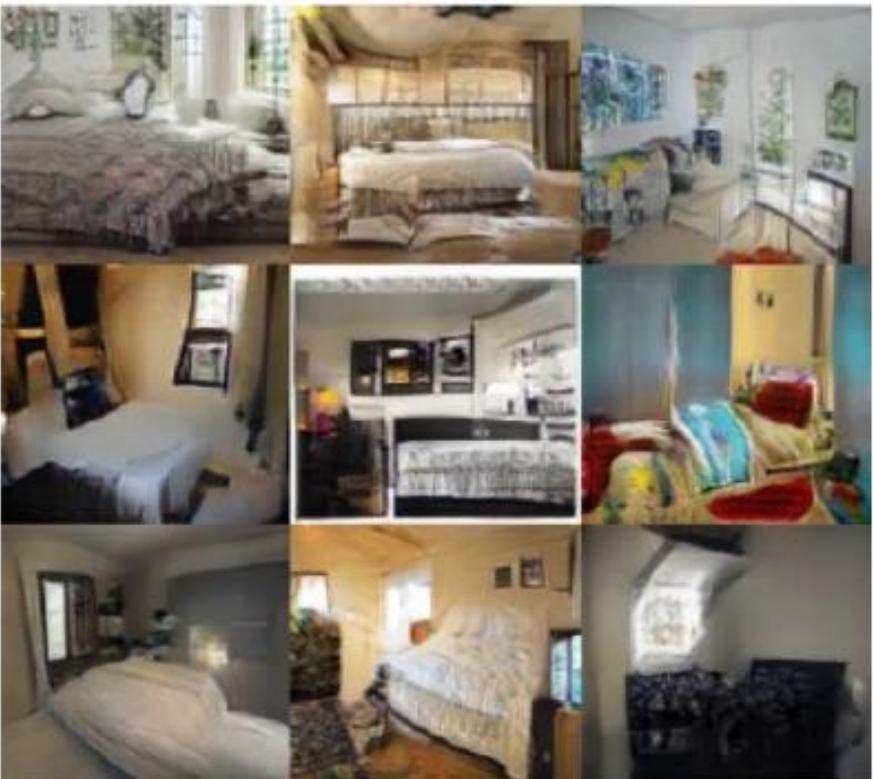


# Vector Arithmetic

Interpolation of view changes



# GAN has been a very active research field



LSGAN, Zhu 2017.



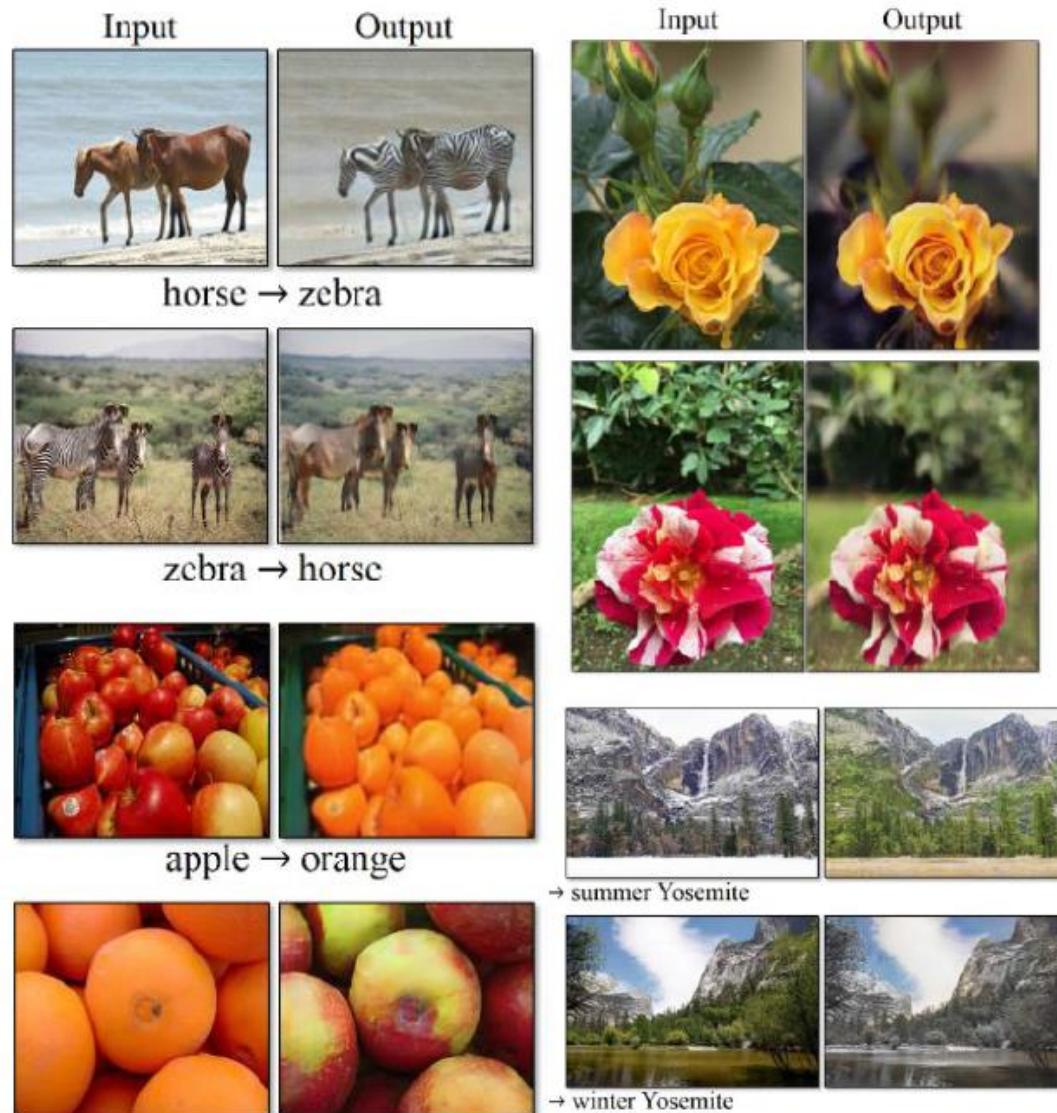
Wasserstein GAN,  
Arjovsky 2017.  
Improved Wasserstein  
GAN, Gulrajani 2017.

# GAN has been a very active research field



# GANs for source-target domain transfer

This can also be used for photo enhancement and data augmentation



CycleGAN. Zhu et al. 2017.

## ... «The GAN ZOO» and <https://github.com/soumith/ganhacks>

this small bird has a pink breast and crown, and black primaries and secondaries.



Reed et al. 2017.

this magnificent fellow is almost all black with a red crest, and white cheek patch.



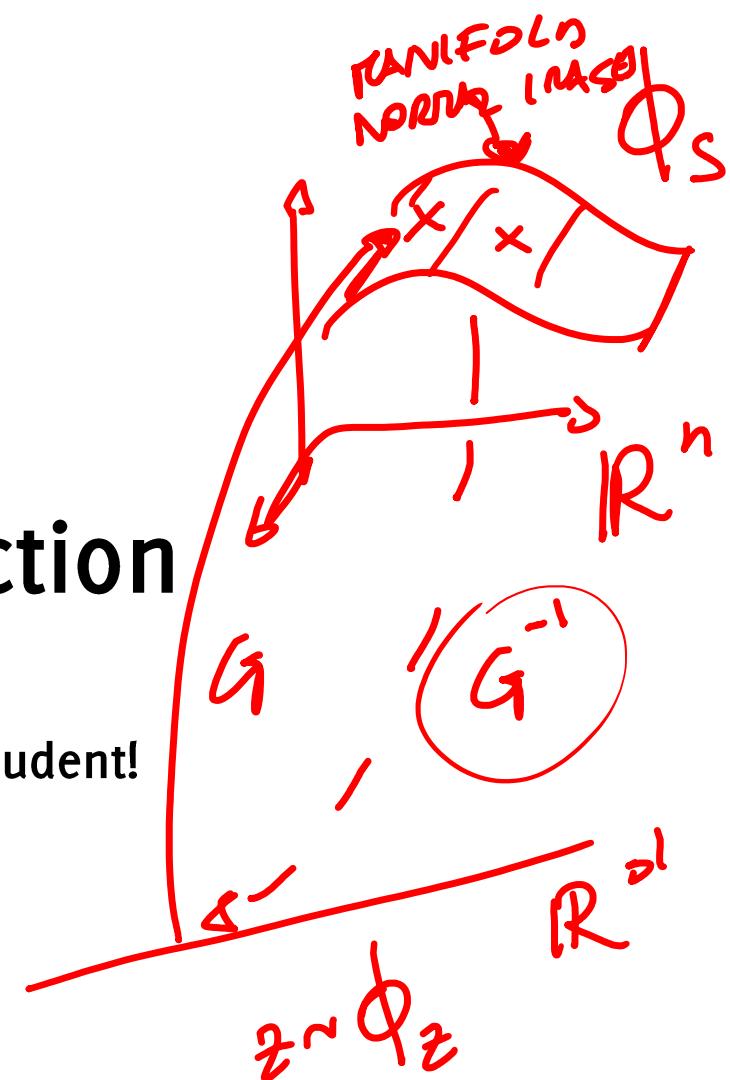
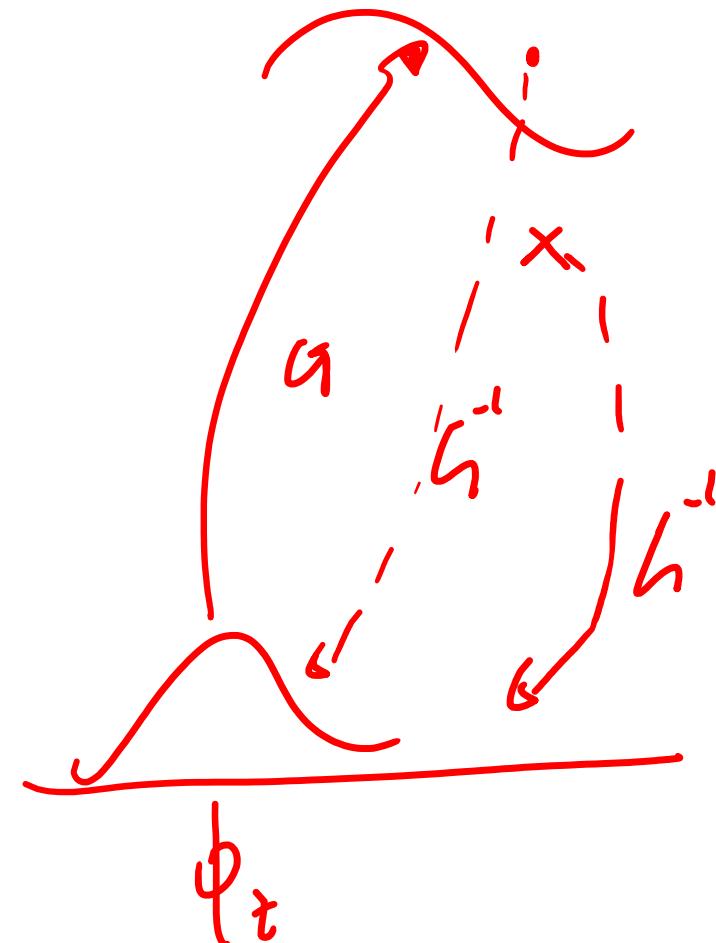
Pix2pix. Isola 2017. Many examples at <https://phillipi.github.io/pix2pix/>

# Generative Adversarial Networks (these people do not exist)



# GAN for Anomaly Detection

Thanks to Stefano Pecchia, former AN2DL student!



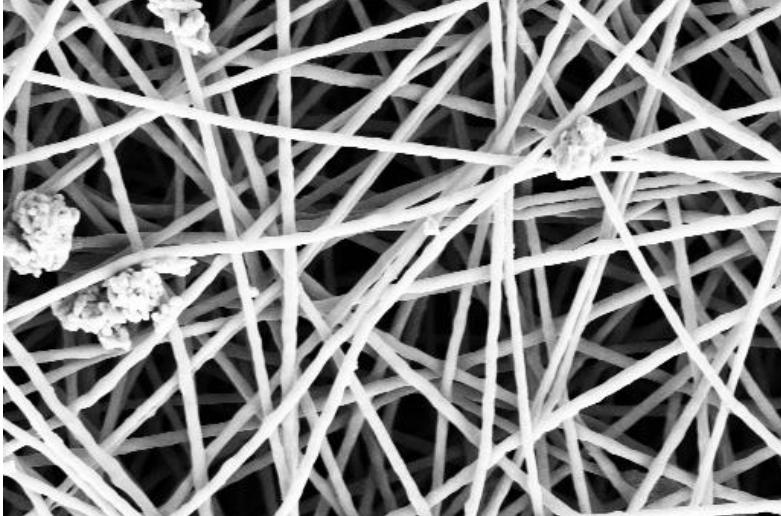
# Anomaly Detection in images

Let  $s$  be an image defined over the pixel domain  $\mathcal{X} \subset \mathbb{Z}^2$ ,

let  $c \in \mathcal{X}$  be a pixel and  $s(c)$  the corresponding intensity.

Our goal is to locate any **anomalous region** in  $s$ , i.e. **estimating the unknown anomaly mask  $\Omega$**  defined as

$$TR = \{\text{normal regions}\} \quad \Omega(c) = \begin{cases} 0 & \text{if } c \text{ falls in a normal region} \\ 1 & \text{if } c \text{ falls in an anomalous region} \end{cases}$$



# Anomaly Detection in images

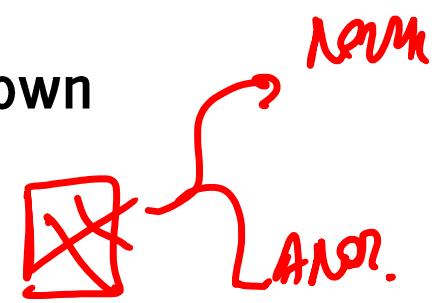
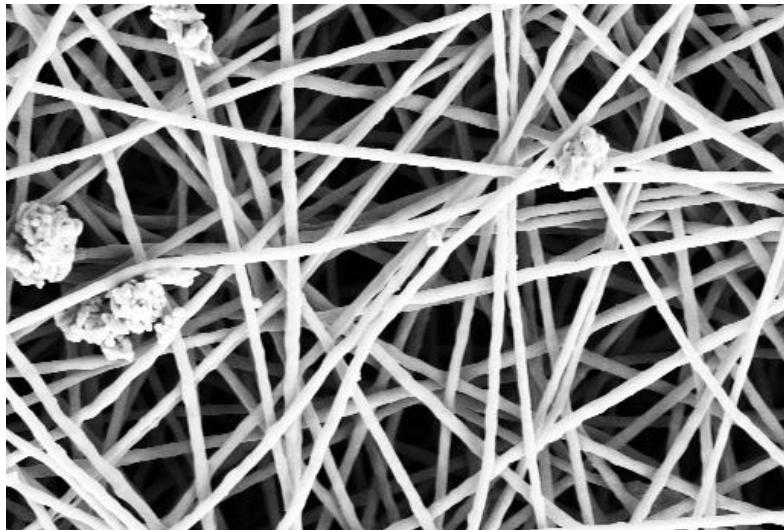
Let  $s$  be an image defined over the pixel domain  $\mathcal{X} \subset \mathbb{Z}^2$ ,

let  $c \in \mathcal{X}$  be a pixel and  $s(c)$  the corresponding intensity.

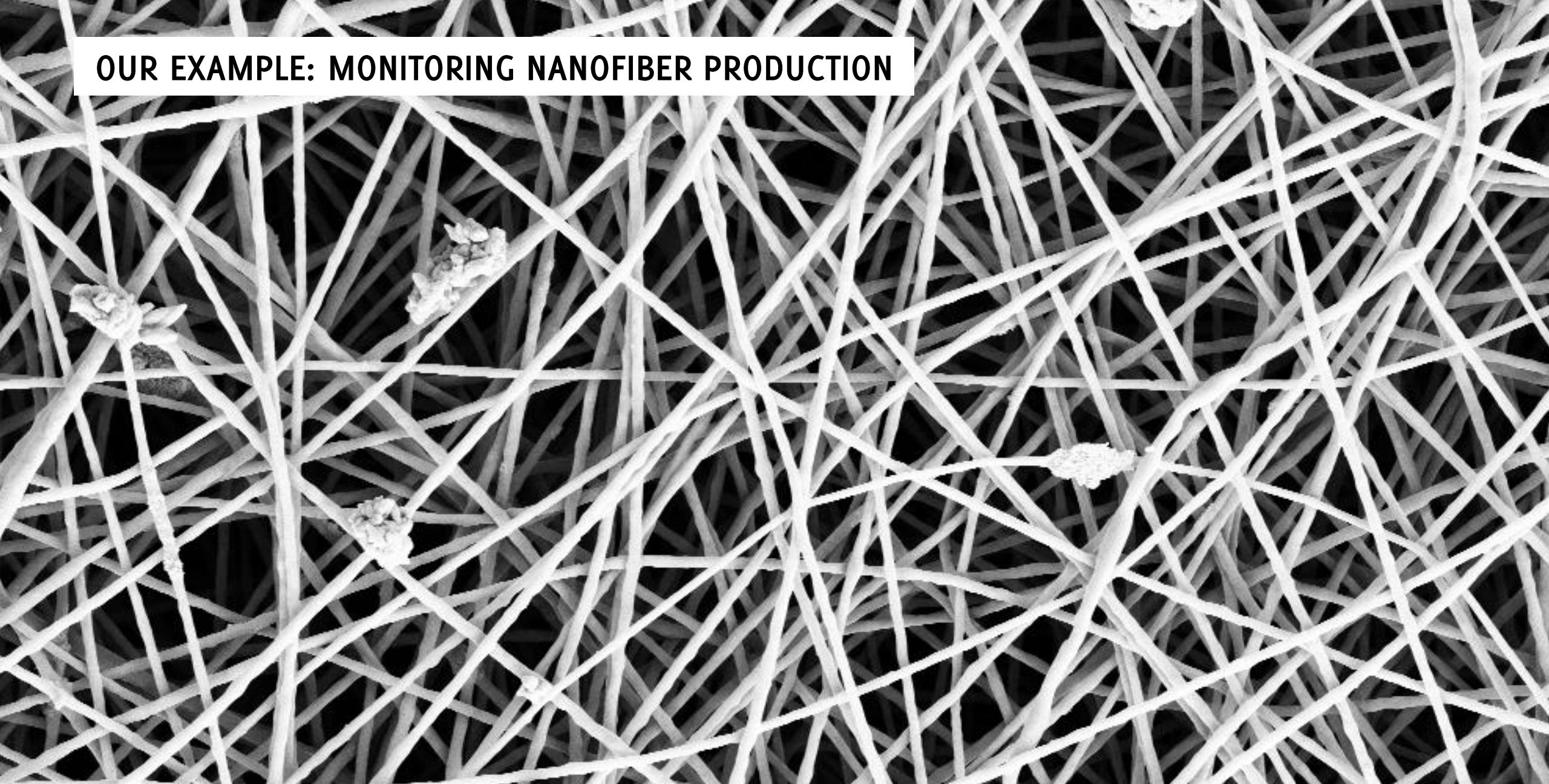
Our goal is to locate any **anomalous region** in  $s$ , i.e. estimating the unknown **anomaly mask  $\Omega$**  defined as

$$\Omega(c) = \begin{cases} 0 & \text{if } c \text{ falls in a normal region} \\ 1 & \text{if } c \text{ falls in an anomalous region} \end{cases}$$

$s$

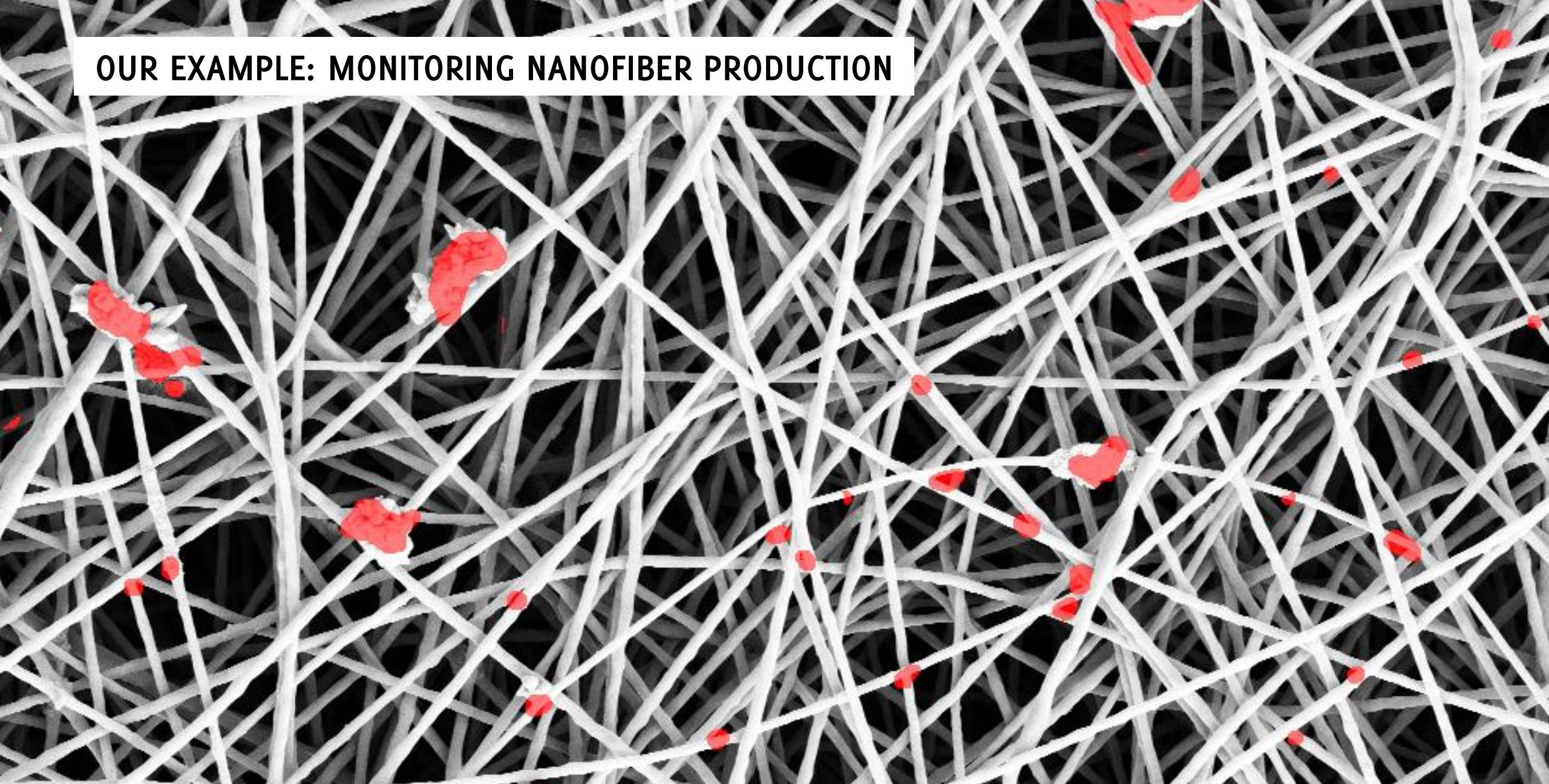


## OUR EXAMPLE: MONITORING NANOFIBER PRODUCTION



Carrera D., Manganini F., Boracchi G., Lanzarone E. "Defect Detection in SEM Images of Nanofibrous Materials", IEEE Transactions on Industrial Informatics 2017, 11 pages, doi:10.1109/TII.2016.2641472

## OUR EXAMPLE: MONITORING NANOFIBER PRODUCTION



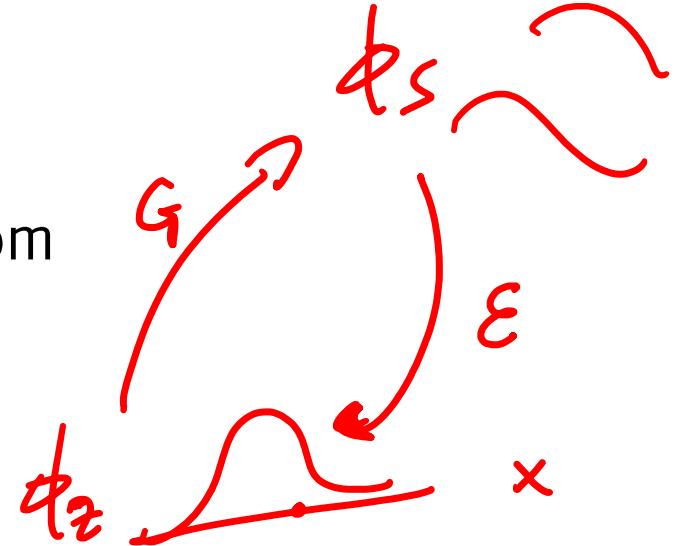
Carrera D., Manganini F., Boracchi G., Lanzarone E. "Defect Detection in SEM Images of Nanofibrous Materials", IEEE Transactions on Industrial Informatics 2017, 11 pages, doi:10.1109/TII.2016.2641472

# GANs and Anomaly Detection

*NOISE IMAGE ONLY / PATCHES*

A Generator  $G$  trained by a GAN provides already a mapping from

- The space of random vectors  $z \sim \phi_z$
- The manifold where images live  $s \sim \phi_s$



Thus, If we could invert the GAN, we would have already an AD model

Given a test image  $s \rightarrow G^{-1}(s) \rightarrow \phi_z(G^{-1}(s))$  would be an anomaly score

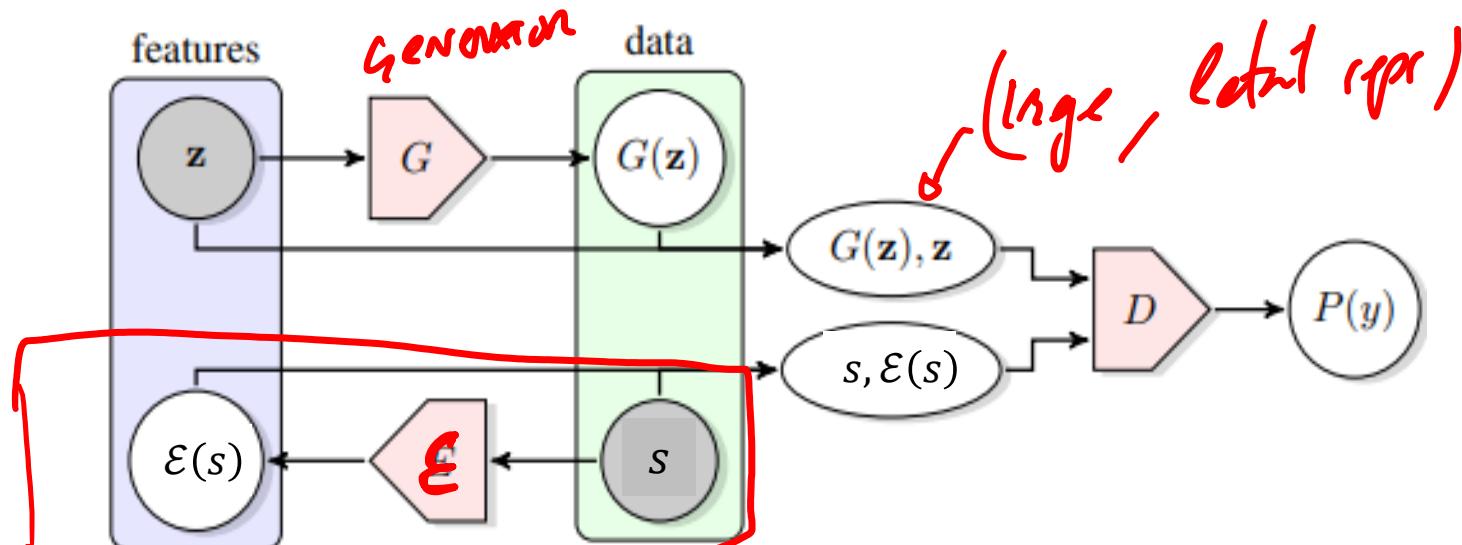
Unfortunately, it is not possible to invert  $G$ ... some neural network need to be trained for this purpose!

# BidirectionalGANs (BiGANs)

The BiGAN adds an encoder  $E$  to the adversarial game which

- Brings an image back to the space of “noise vectors”
- Can be used to reconstruct an input image  $s$  (as in autoencoders)  $G(E(s))$
- The discriminator  $\mathcal{D}$  takes as input (image, latent repr.) as in conditional GAN

$$\min_{G,E} \max_{\mathcal{D}} V(\mathcal{D}, E, G)$$
$$V(\mathcal{D}, E, G) = \mathbb{E}_{s \sim \phi_s} [\log \mathcal{D}(s, E(s))] + \mathbb{E}_{z \sim \phi_z} [1 - \log \mathcal{D}(G(z), z)]$$



# BidirectionalGANs (BiGANs) and Anomaly Detection

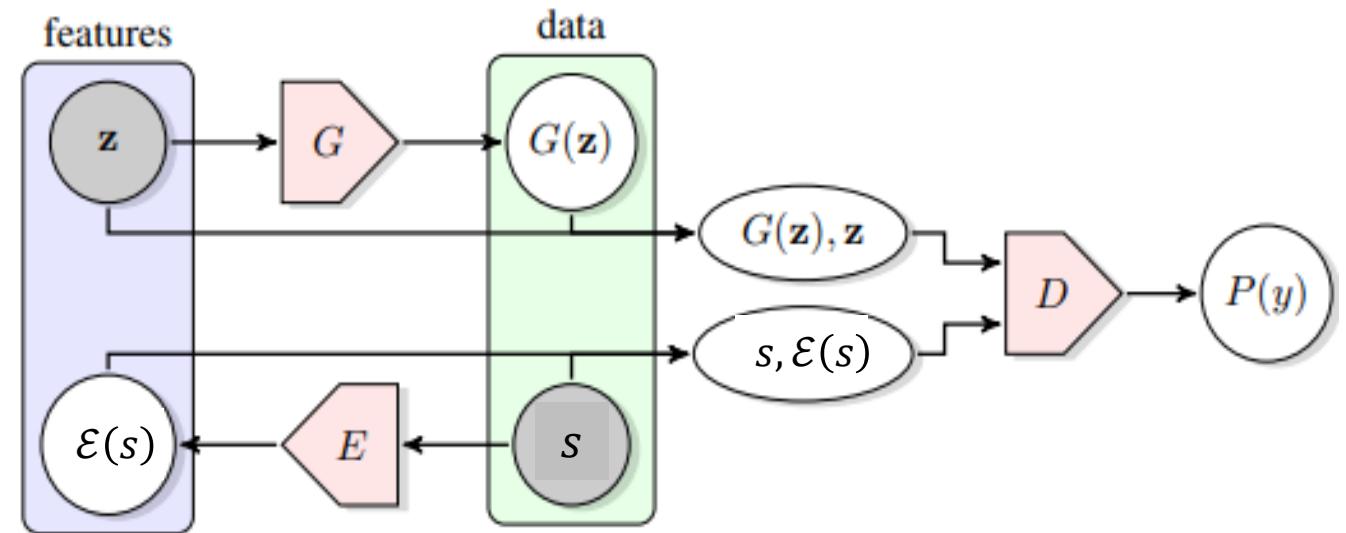
In principle, the encoder  $\mathcal{E}(\cdot)$  can be used for anomaly detection by computing the likelihood of  $\phi_z(\mathcal{E}(s))$  and consider as anomalous all the images  $s$  corresponding to a low likelihood (provided that  $\phi_z$  was not a uniform distribution)

$$\phi_z(\mathcal{E}(s)) \quad \text{likelihood}$$

Another option is to use the posterior of the discriminator as anomaly score

$$(\text{standard GAN}) \quad D(s) \quad \mathcal{D}(s, \mathcal{E}(s))$$

since the discriminator will consider the anomalous sample as fake.

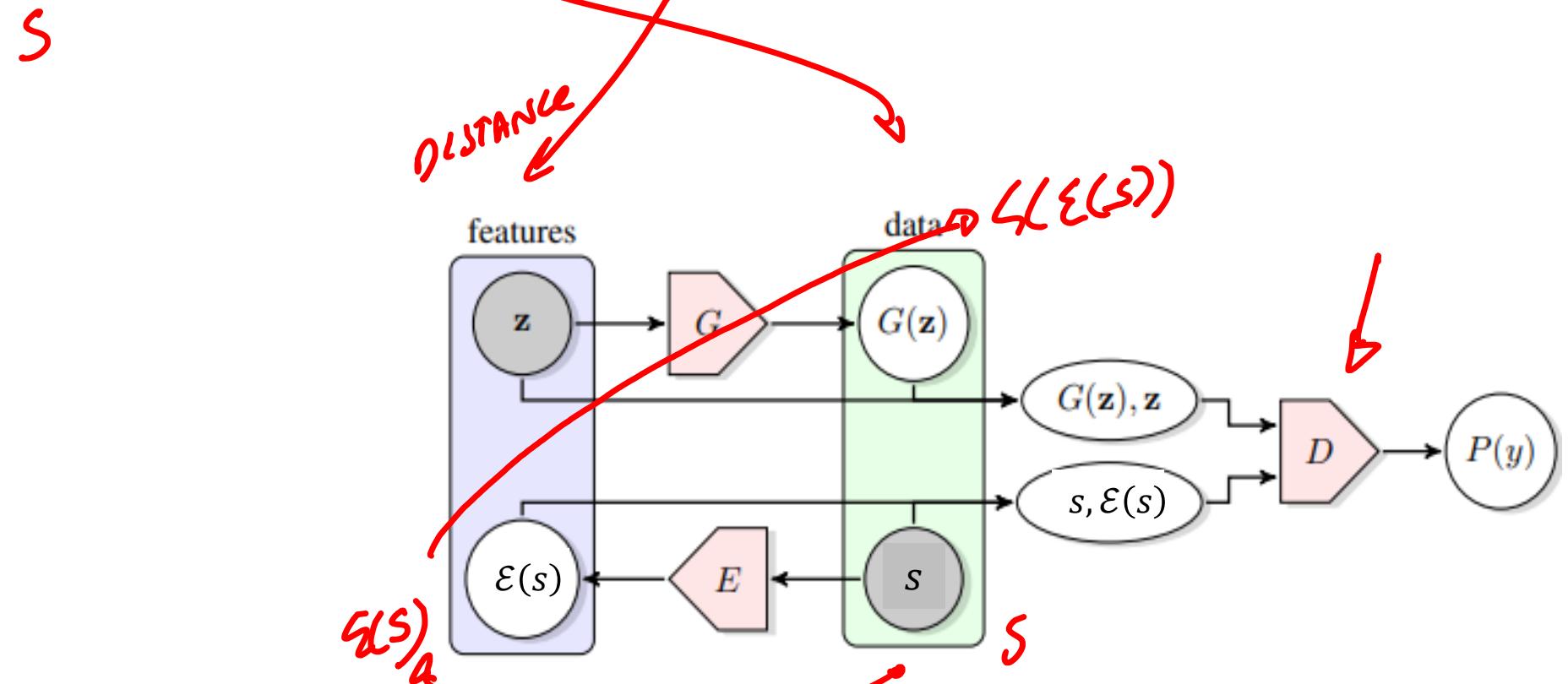


# Anomaly detection with BidirectionalGANs (BiGANs)

However, there are more effective anomaly scores

$$A(s) = (1 - \alpha) \left\| G(\mathcal{E}(s)) - s \right\|_2 + \alpha \left\| f(D(s, \mathcal{E}(s))) - f(D(G(\mathcal{E}(s)), \mathcal{E}(s))) \right\|_2$$

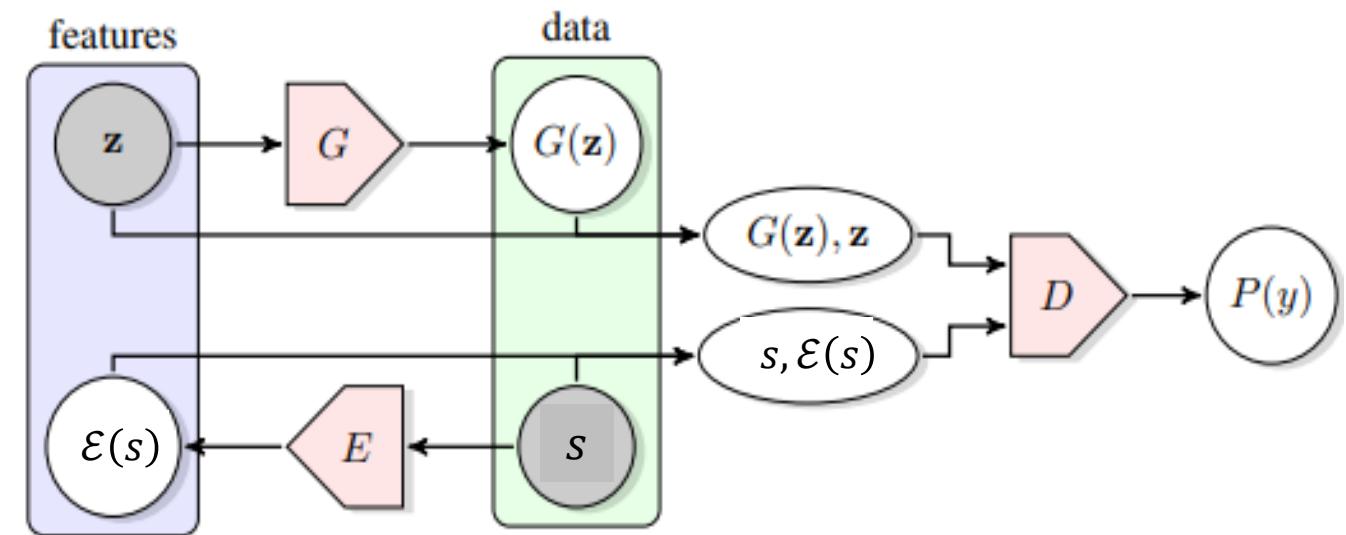
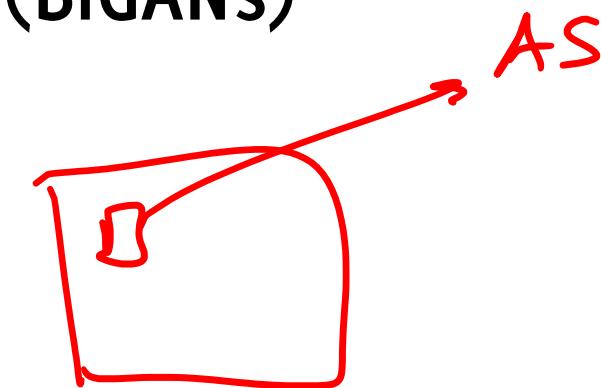
Reconstruction Loss      Distance among latent representations of  $\mathcal{D}$ .  
 $f$  is the operation of extracting a latent representation



# Anomaly detection with BidirectionalGANs (BiGANs)

## Limitations

- Image-wise / patch-wise training and testing
- Little stability during training
- No way to promote better quality of reconstructed images

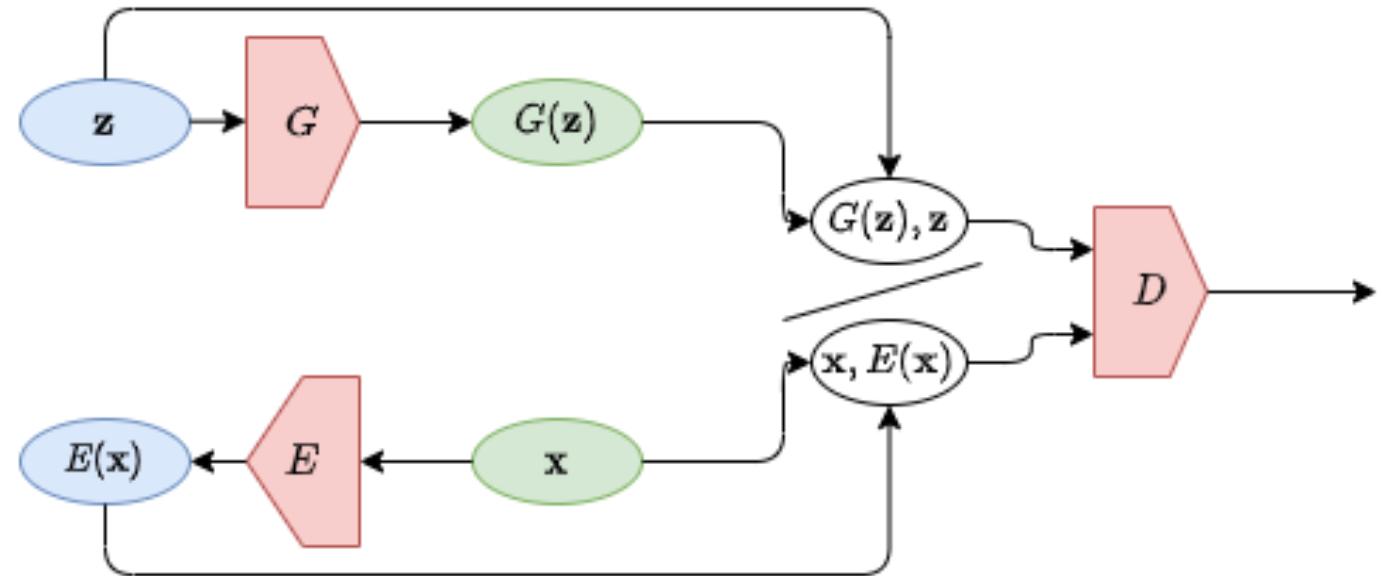


# Fully Convolutional Anomaly Detection by GANs

## Training

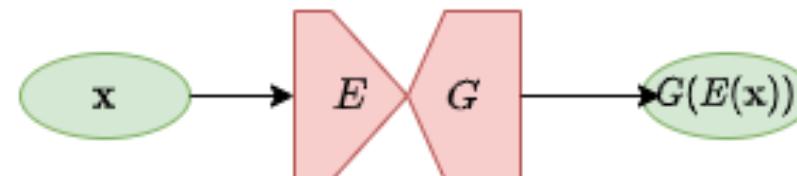
- All the layers are made fully convolutional (much more efficient processing)
- LS-losses used to train the model (this improves stability)

## Adversarial Loss



## Training

## Reconstruction Penalty



# Fully Convolutional Anomaly Detection by GANs

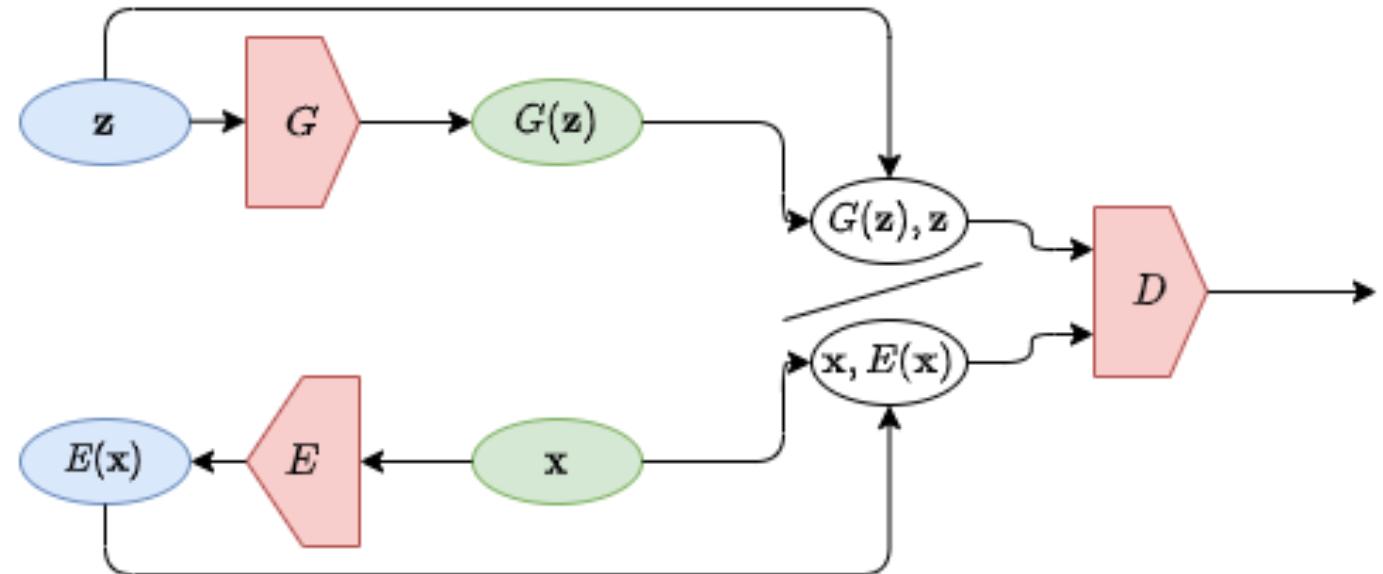
## Inference

- **Anomaly score:** combines
  - I. image reconstruction error
$$\|G(\mathcal{E}(s)) - s\|_2$$
  - II. discriminator loss
$$(\mathcal{D}(s, \mathcal{E}(s)) - 1)^2$$

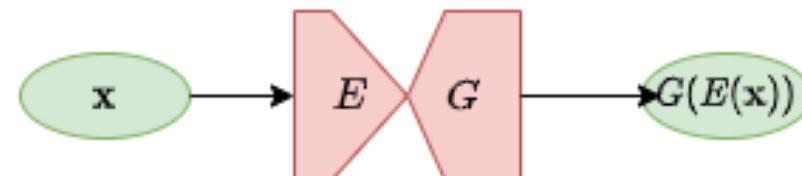
(since normal images are assumed to return 1)

- Possibly also likelihood w.r.t estimated distribution of  $\mathcal{E}(s)$

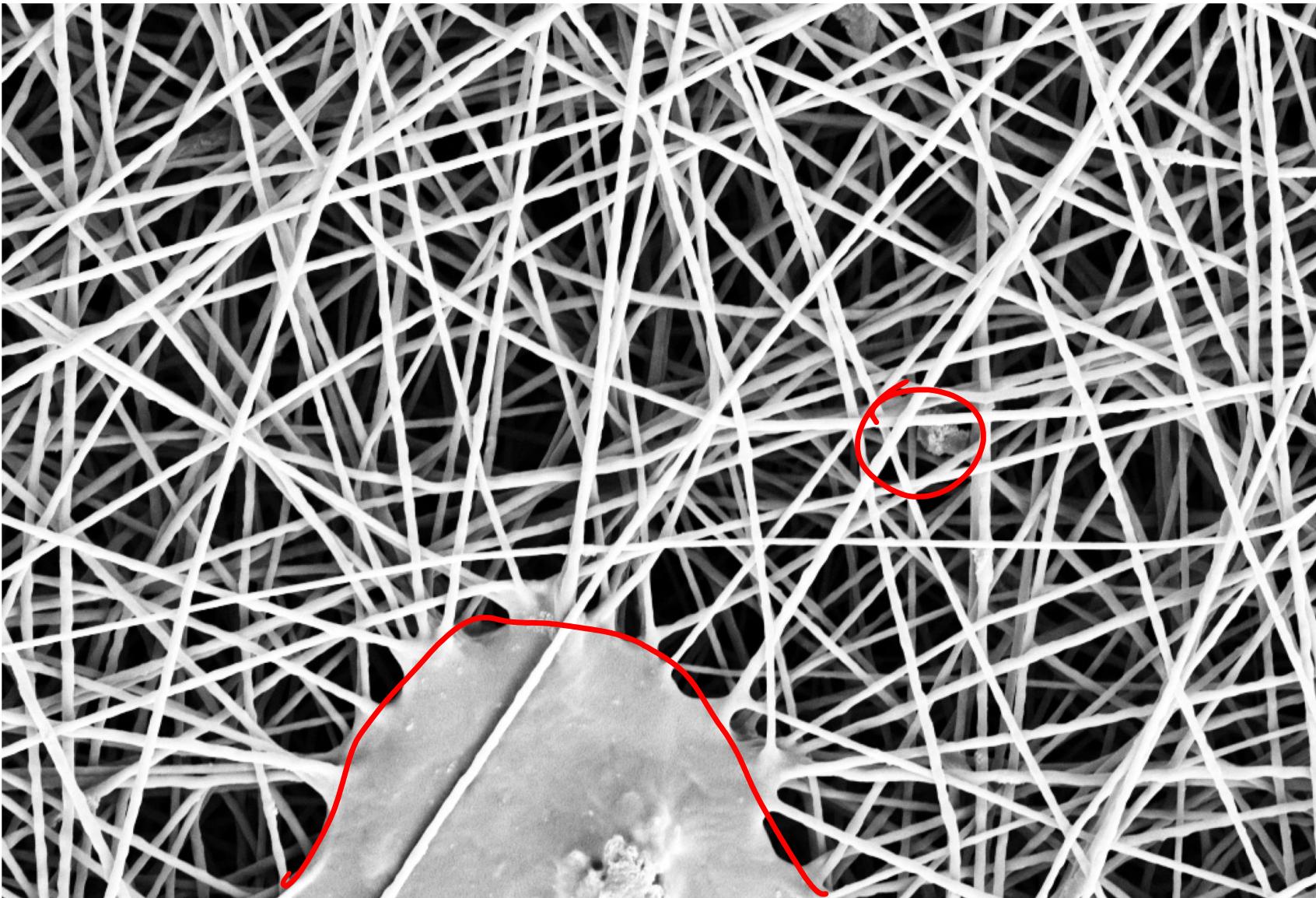
## Adversarial Loss



## Reconstruction Penalty

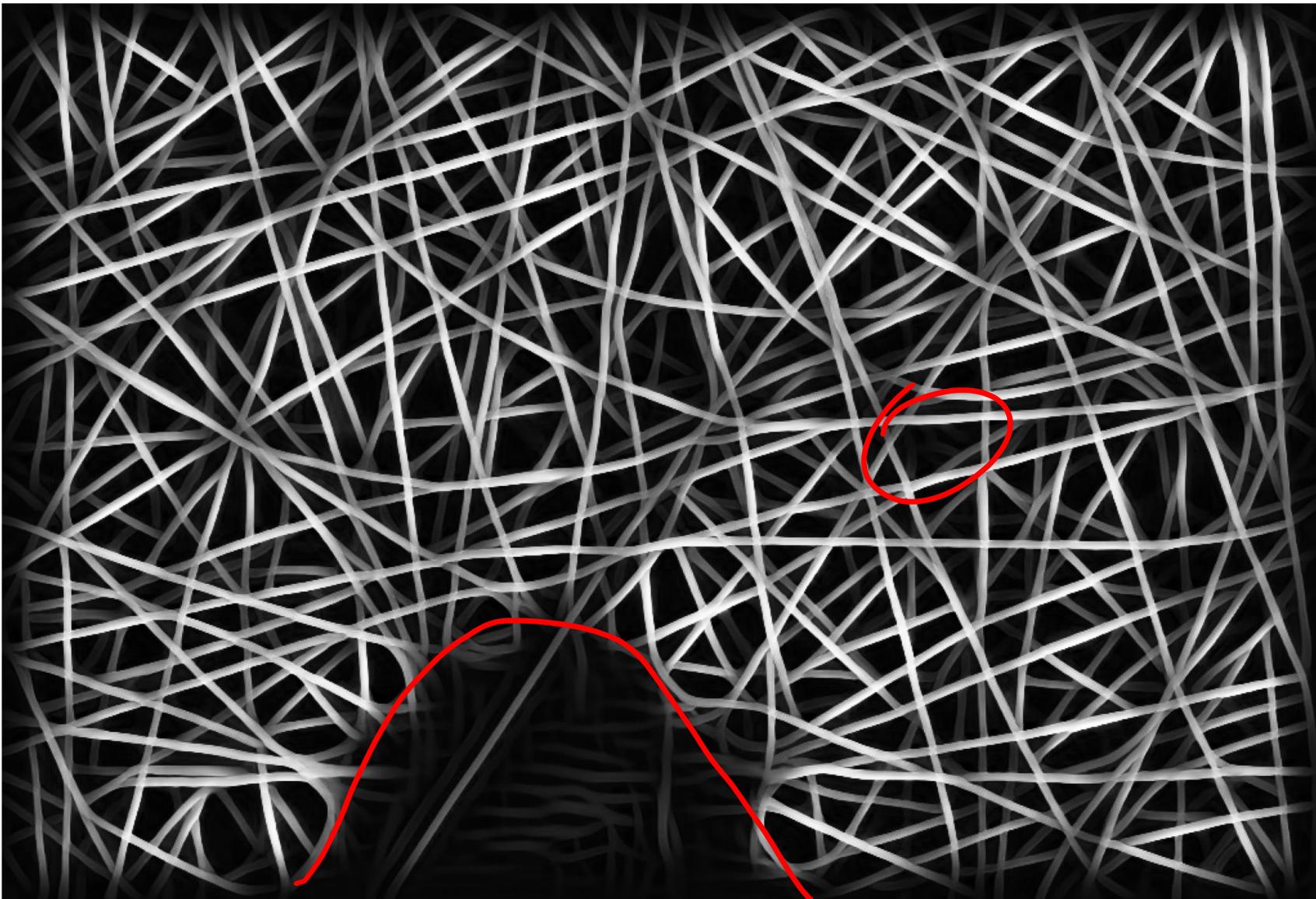


# Input Image

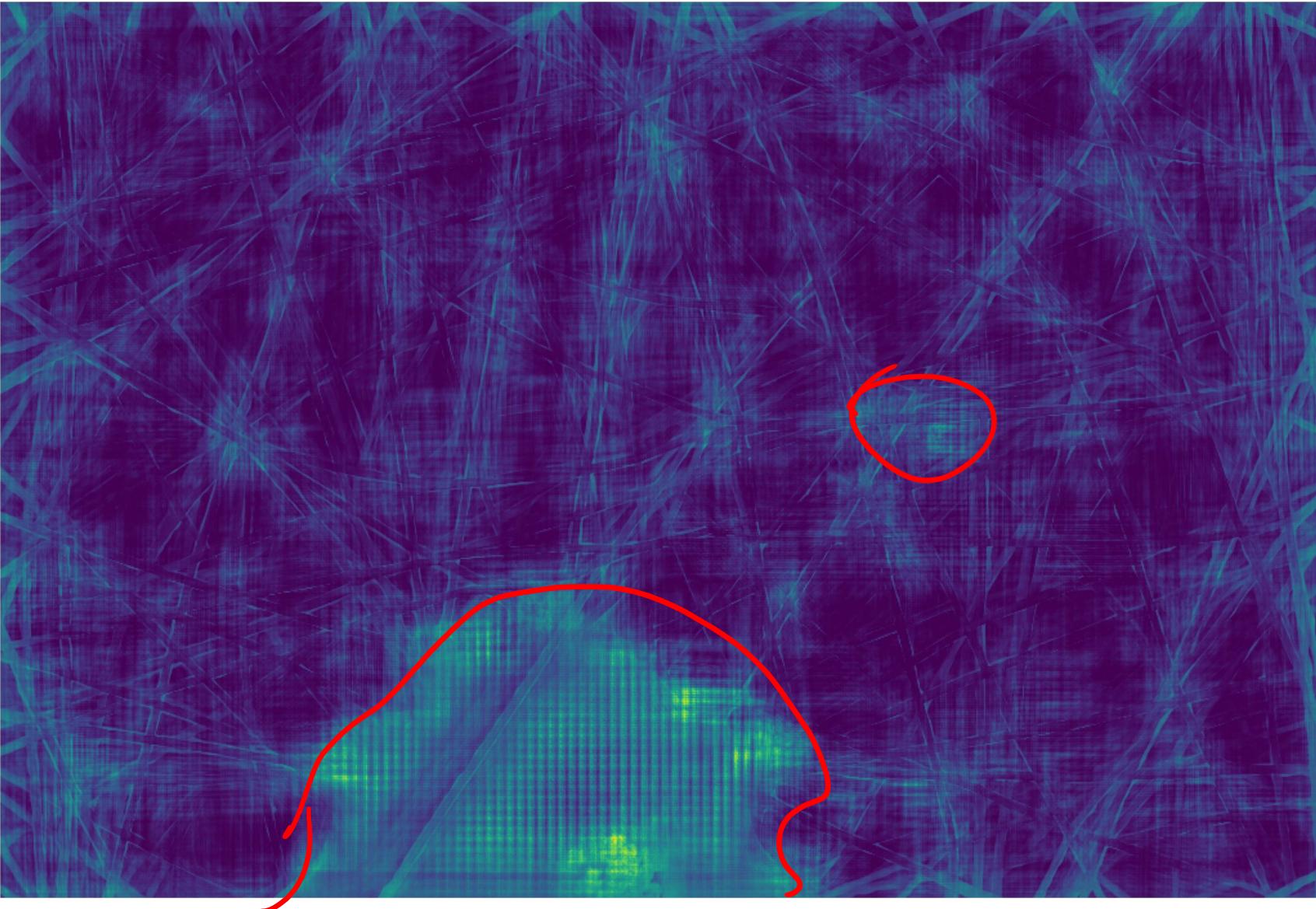


# Reconstruction $\mathcal{G}(\mathcal{E}(s))$

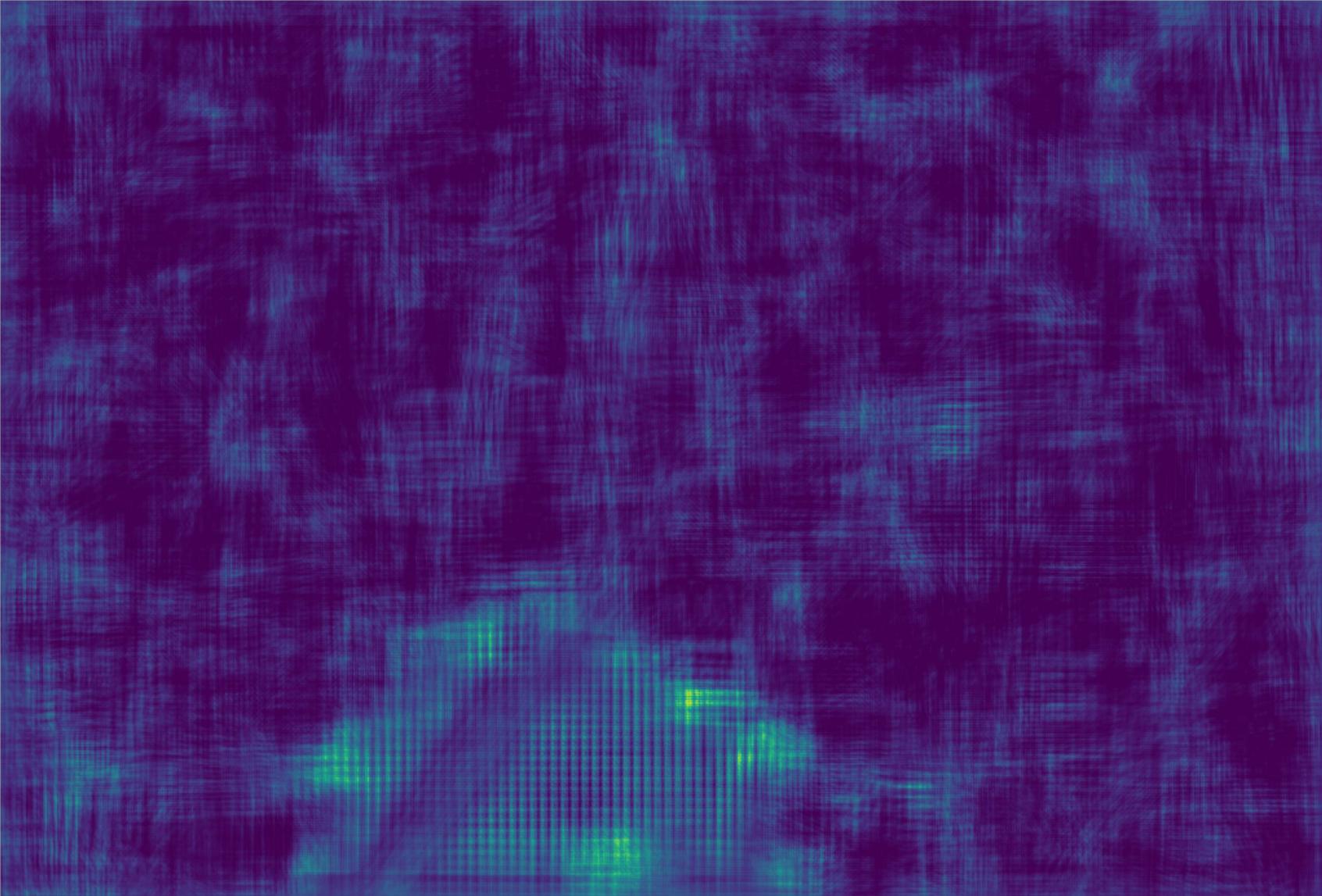
$\mathcal{L}(\mathcal{E}(s))$



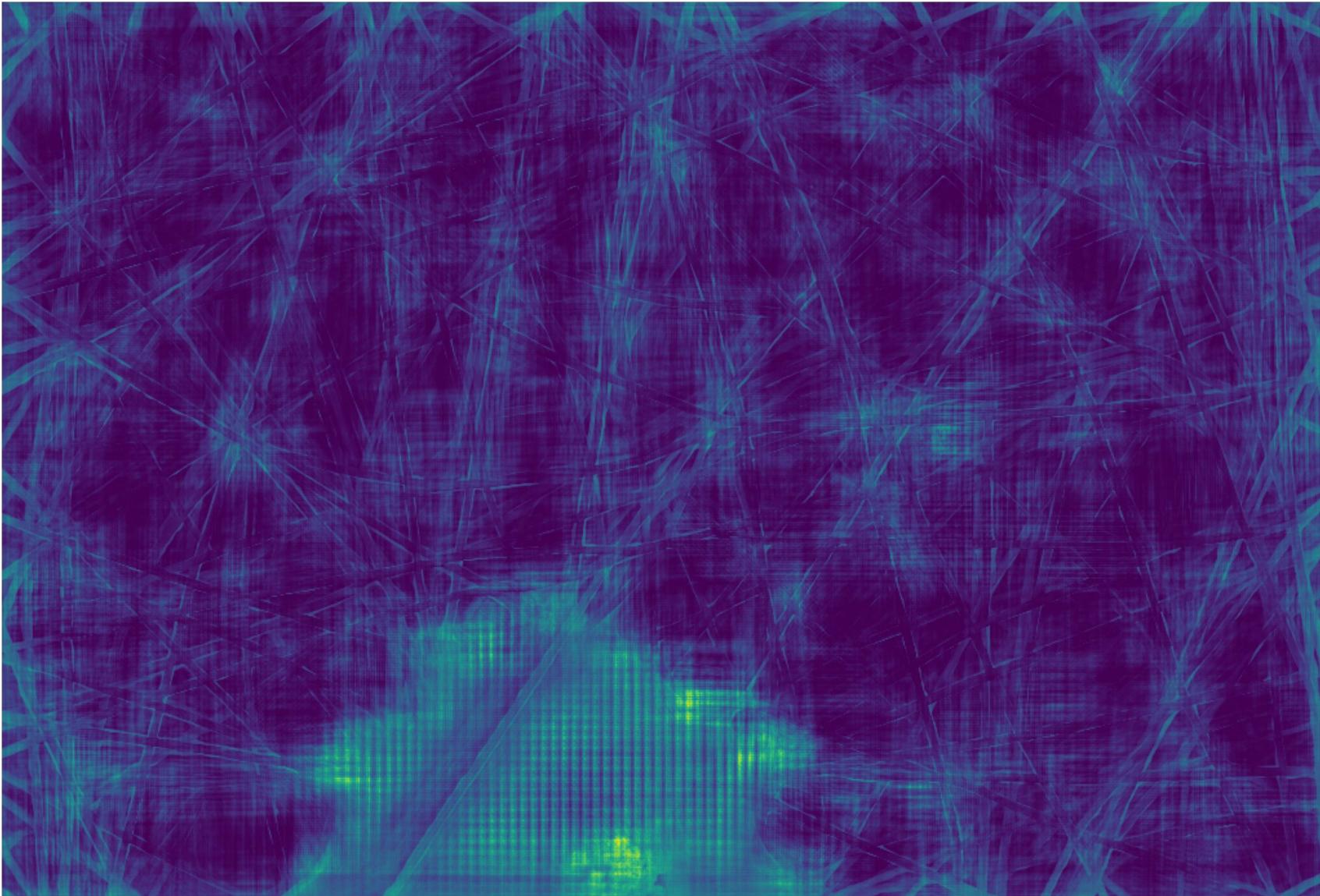
# Reconstruction Loss $\|g(\varepsilon(s)) - s\|_2$



**Discriminator Score**  $(\mathcal{D}(s, \varepsilon(s)) - 1)^2$



$$\text{Anomaly Score } \alpha(\mathcal{D}(s, \mathcal{E}(s)) - 1)^2 + (1 - \alpha)\|\mathcal{G}(\mathcal{E}(s)) - s\|_2$$

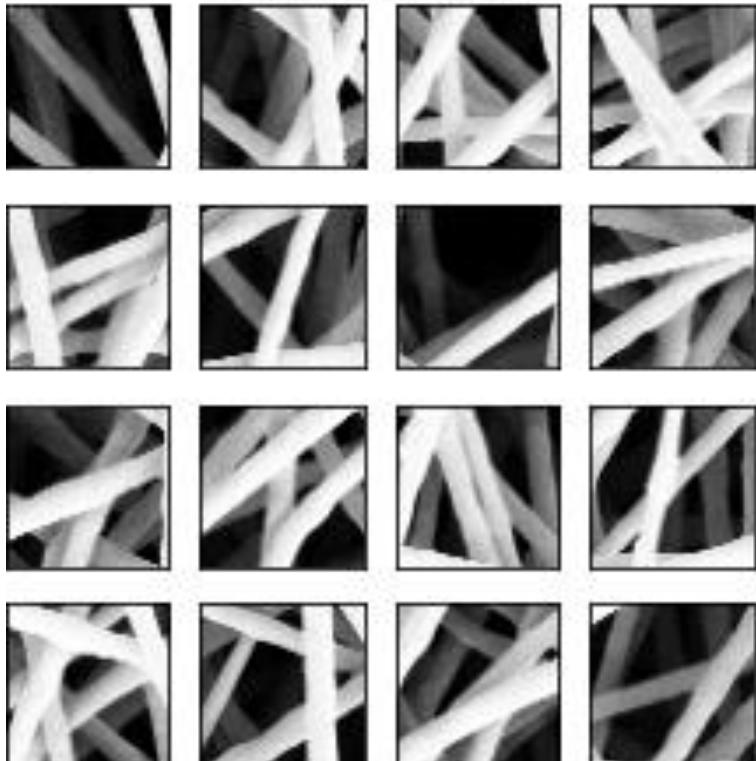


# Normal Image Generation By Our GAN

$z \in \mathbb{R}^{128}$

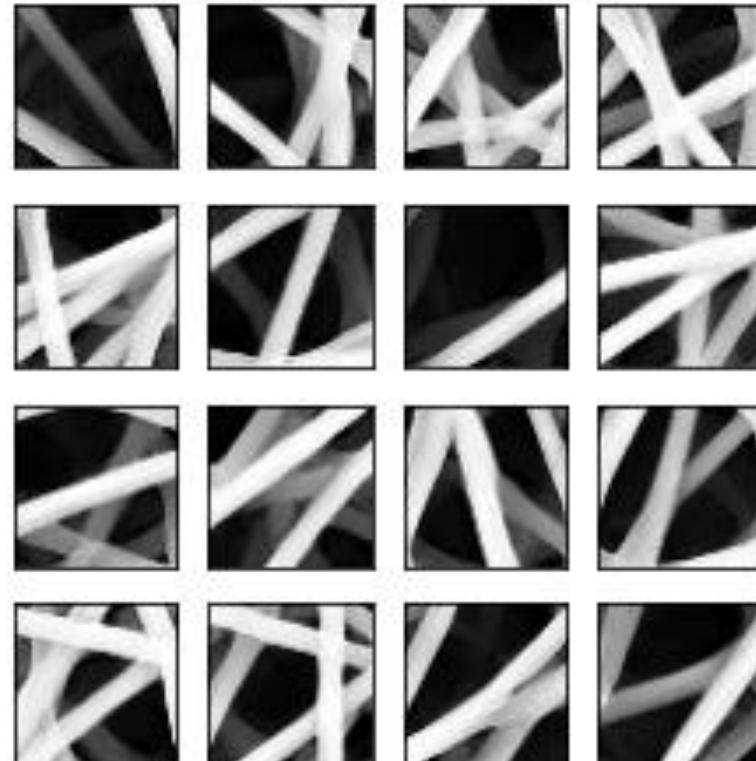
$s$

Original images



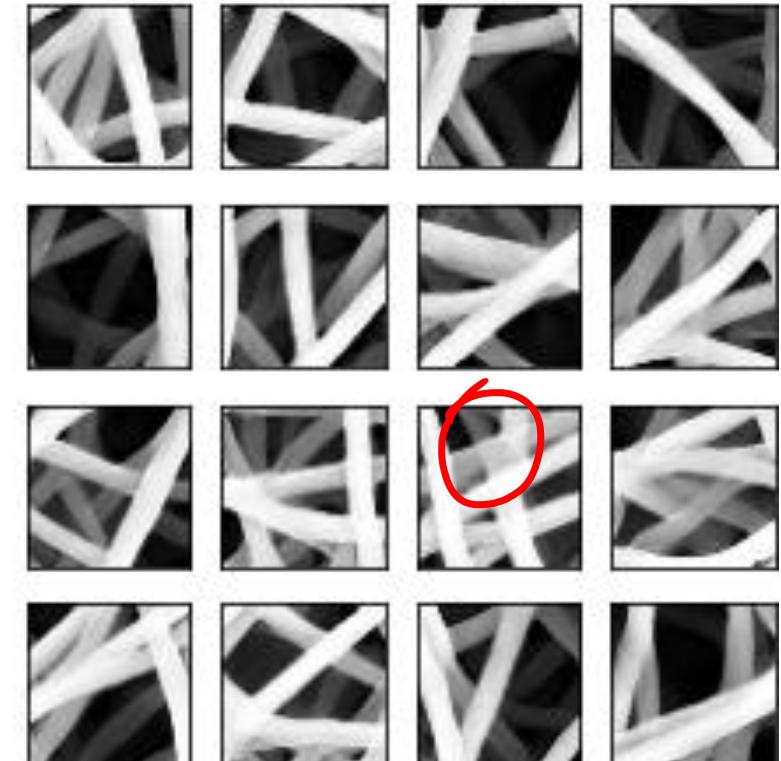
$g(\epsilon(s))$

Reconstructed Images



$g(z)$

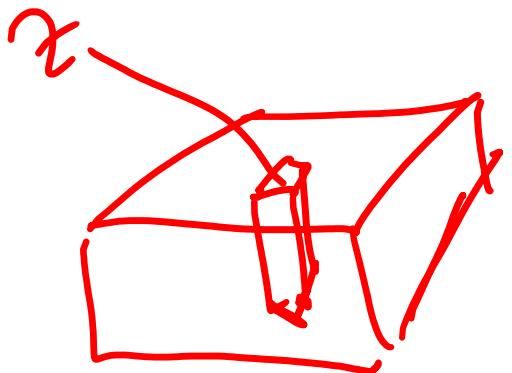
Random Generated Images



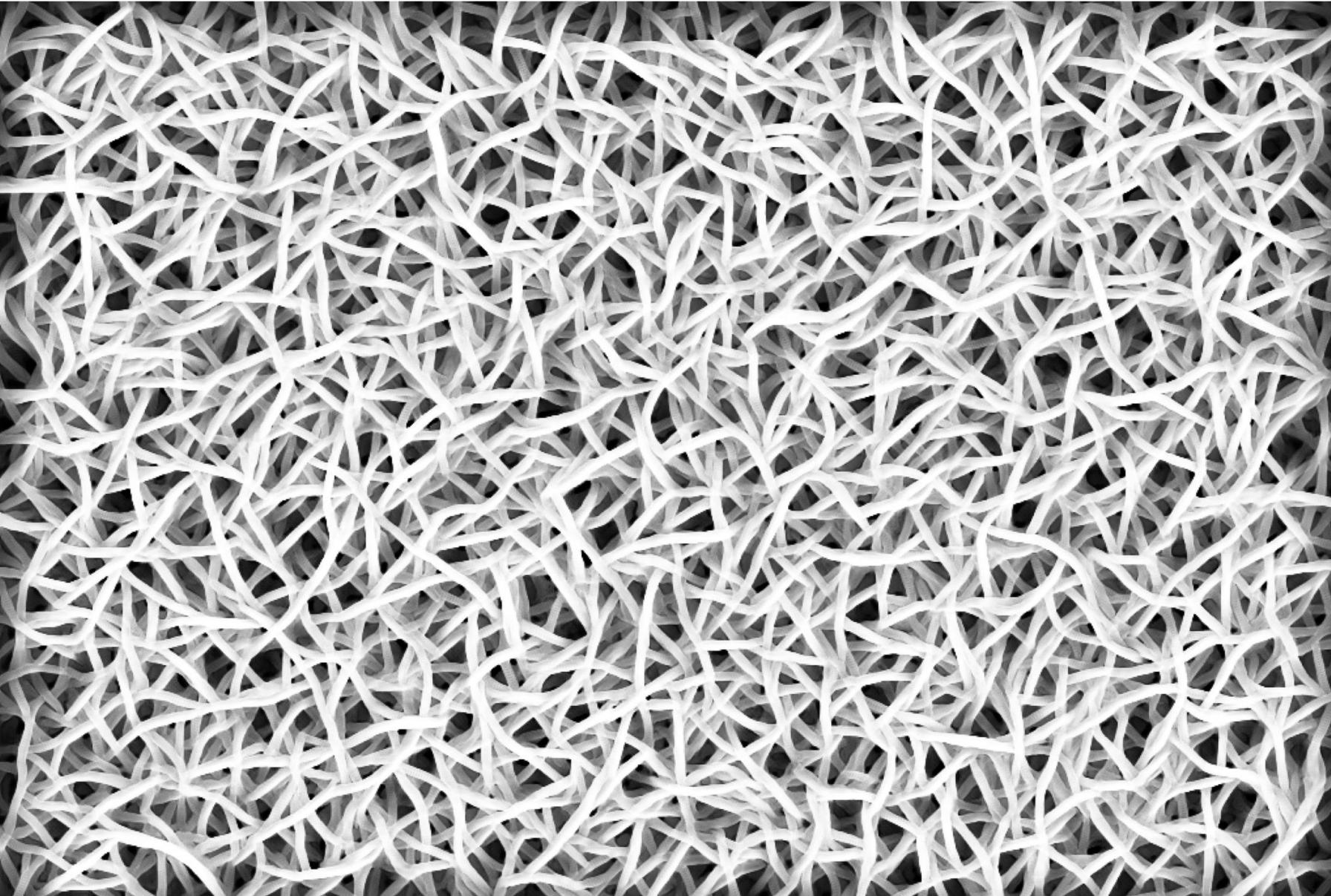
$z \in \mathbb{R}^{128}$

# It is a Generative model!

$$z \in \mathbb{R}^{80 \times 120 \times 128}$$



Local regions are well connected, but the GAN do not enforce a global image structure



# **Mathematical Models and Methods for Image Processing**

Spring 2022, for Mathematical Engineering

**What is this course about?**

# What is this course about?

*It is about **algorithms** for processing **images** and solving image-related problems.*



# What is this course about?

*It is about **algorithms** for processing **images** and solving image-related problems.*

..like denoising



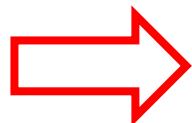
**Who cares about images?**

# Who cares about images?

*Everybody!*

*We will see algorithms solving problems customarily addressed in our phones,*

$$z = y + \eta, \quad \eta \sim \mathcal{N}(0, \sigma^2)$$

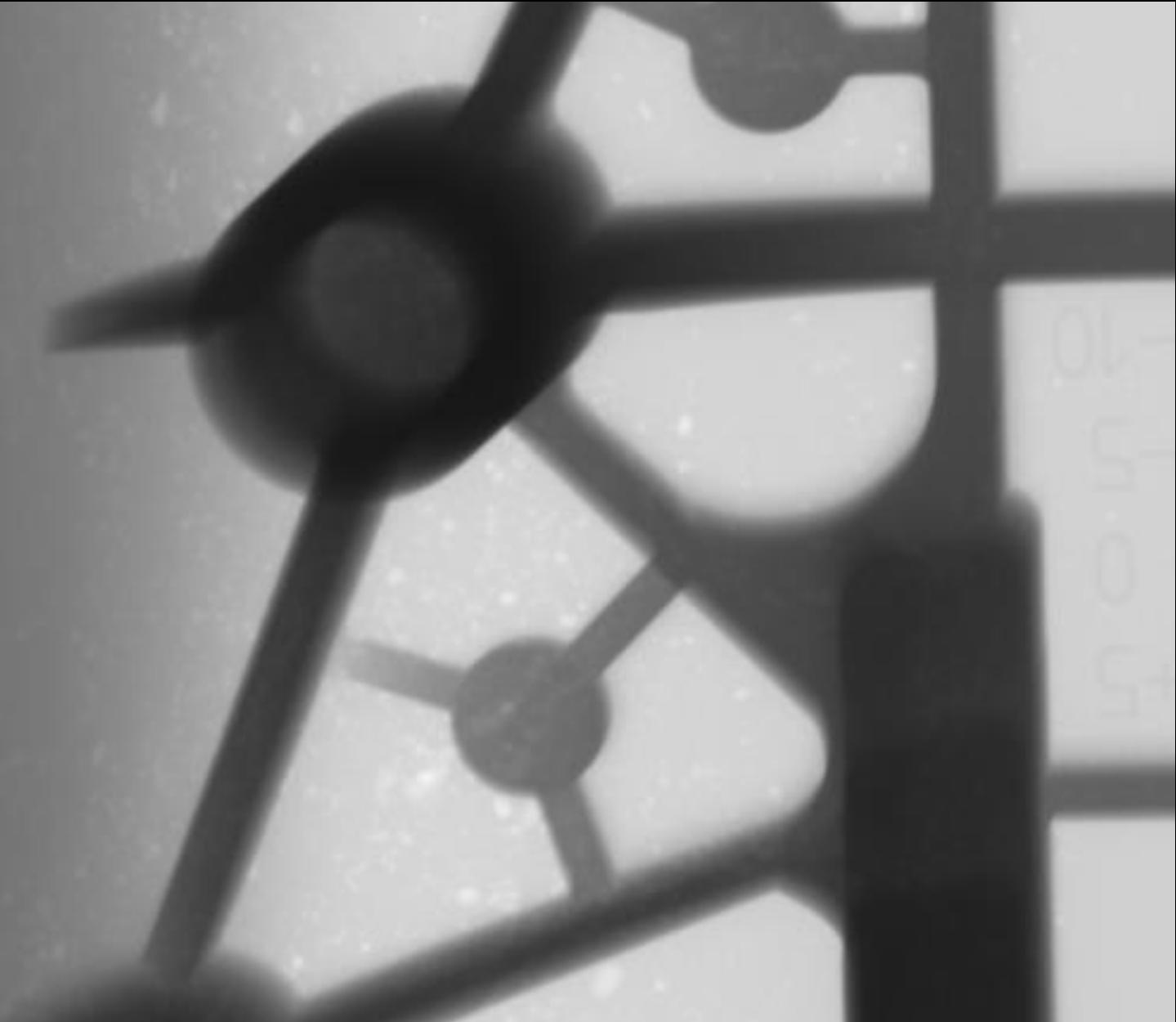


$$\hat{y} \approx y$$

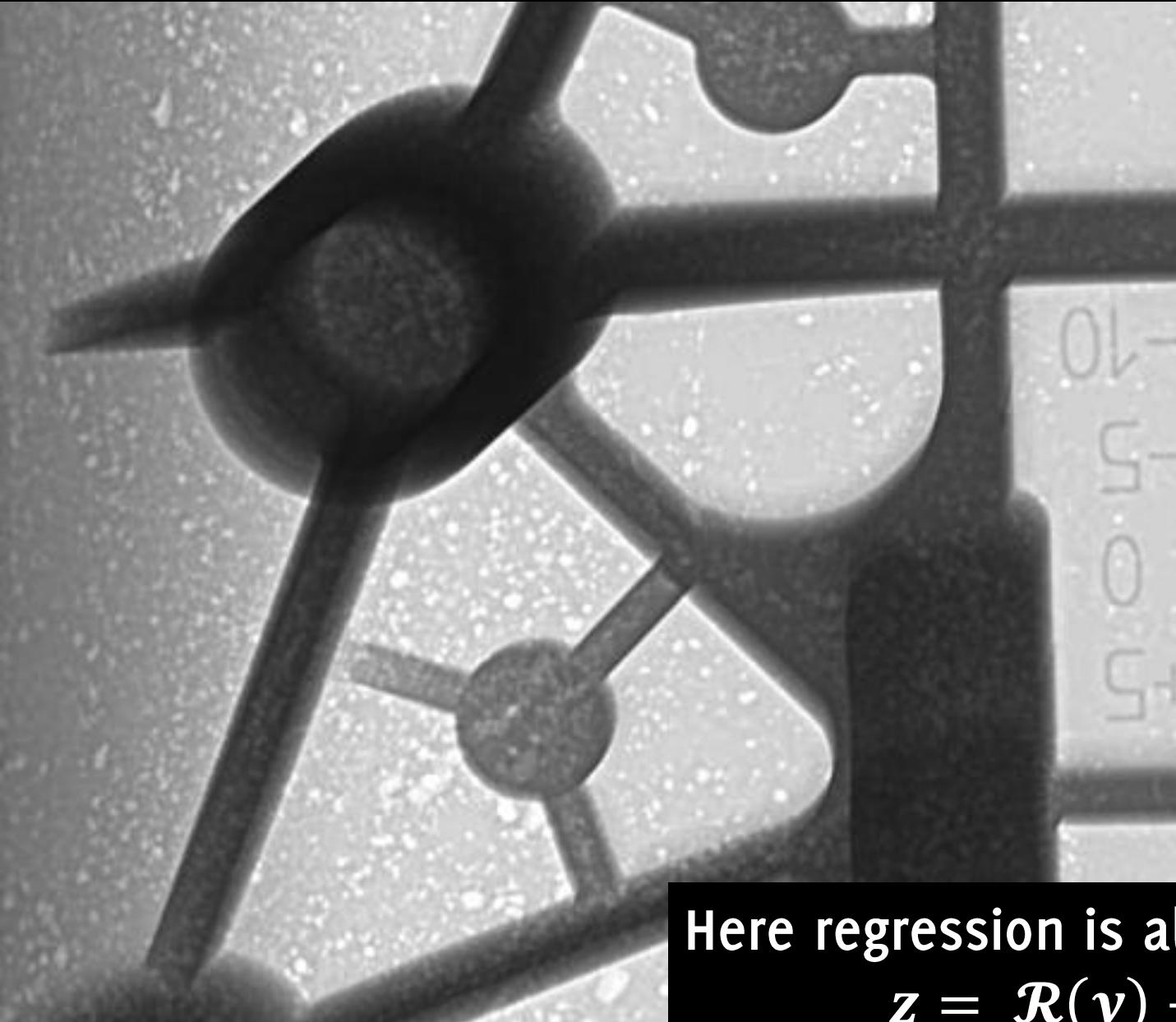


Denoising is a regression problem: given the noisy  $z$ , estimate  $\hat{y}$  close to the unknown  $y$

# Who cares about images? Quality Inspection

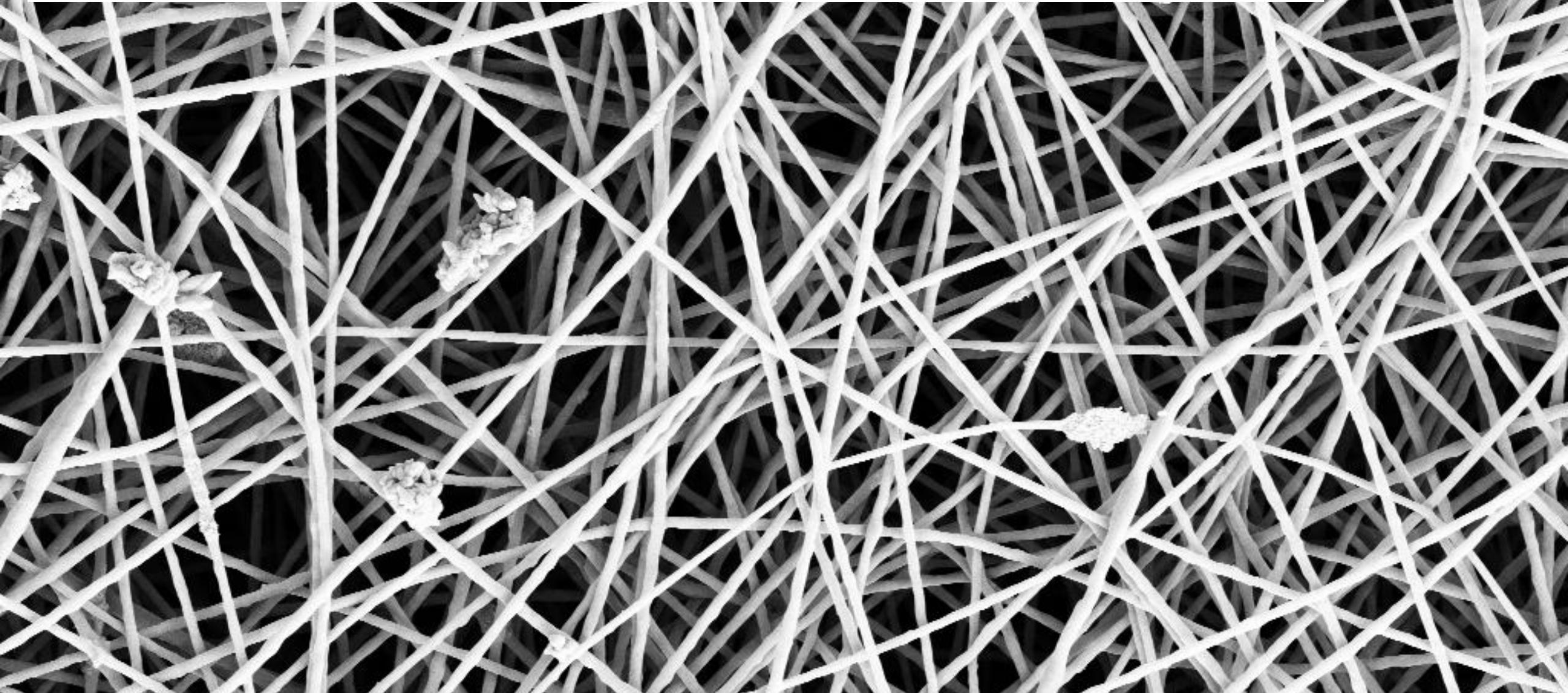


# Who cares about images? Quality Inspection

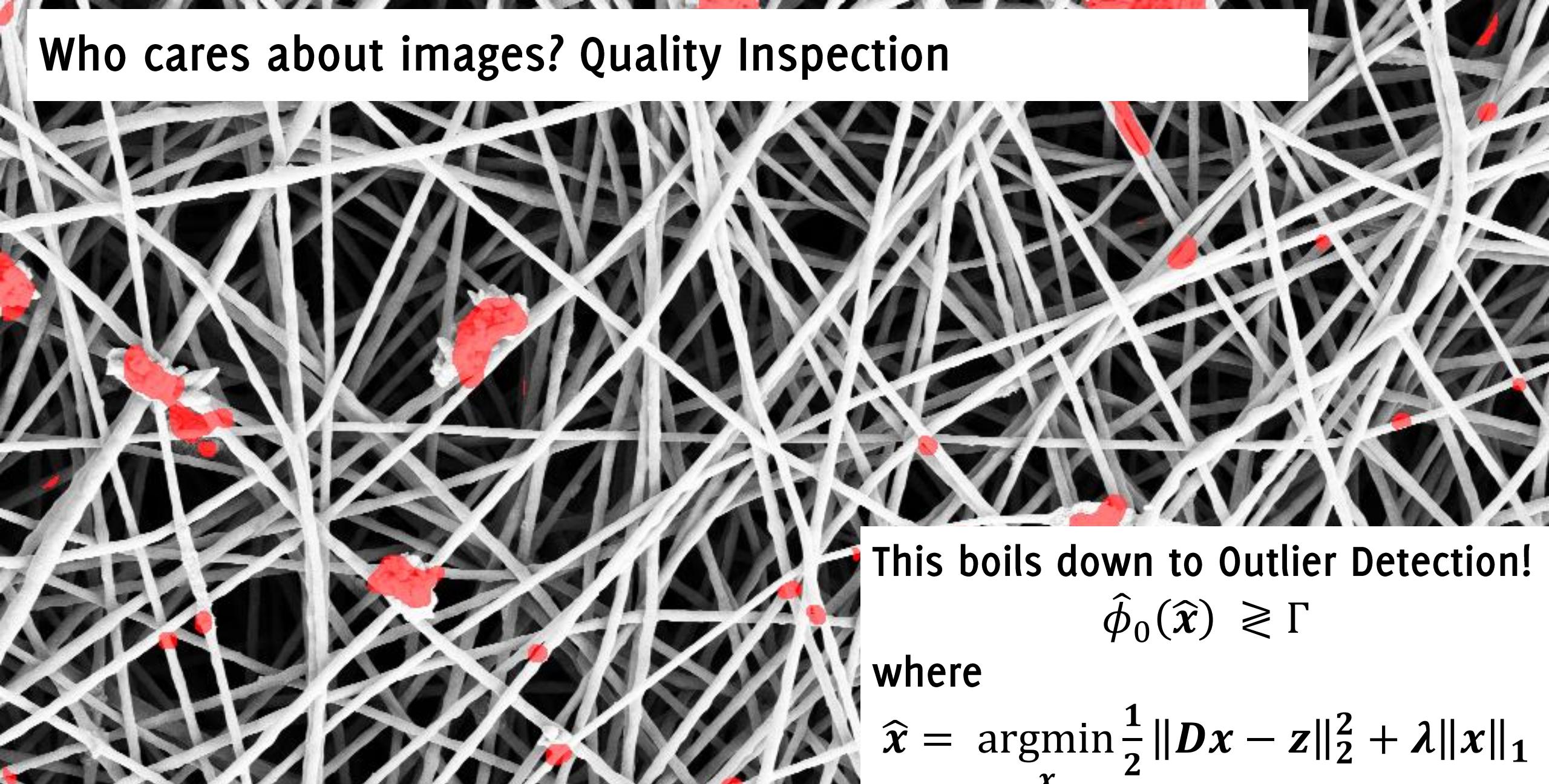


Here regression is also crucial  
 $z = \mathcal{R}(y) + \eta$

# Who cares about images? Quality Inspection



# Who cares about images? Quality Inspection



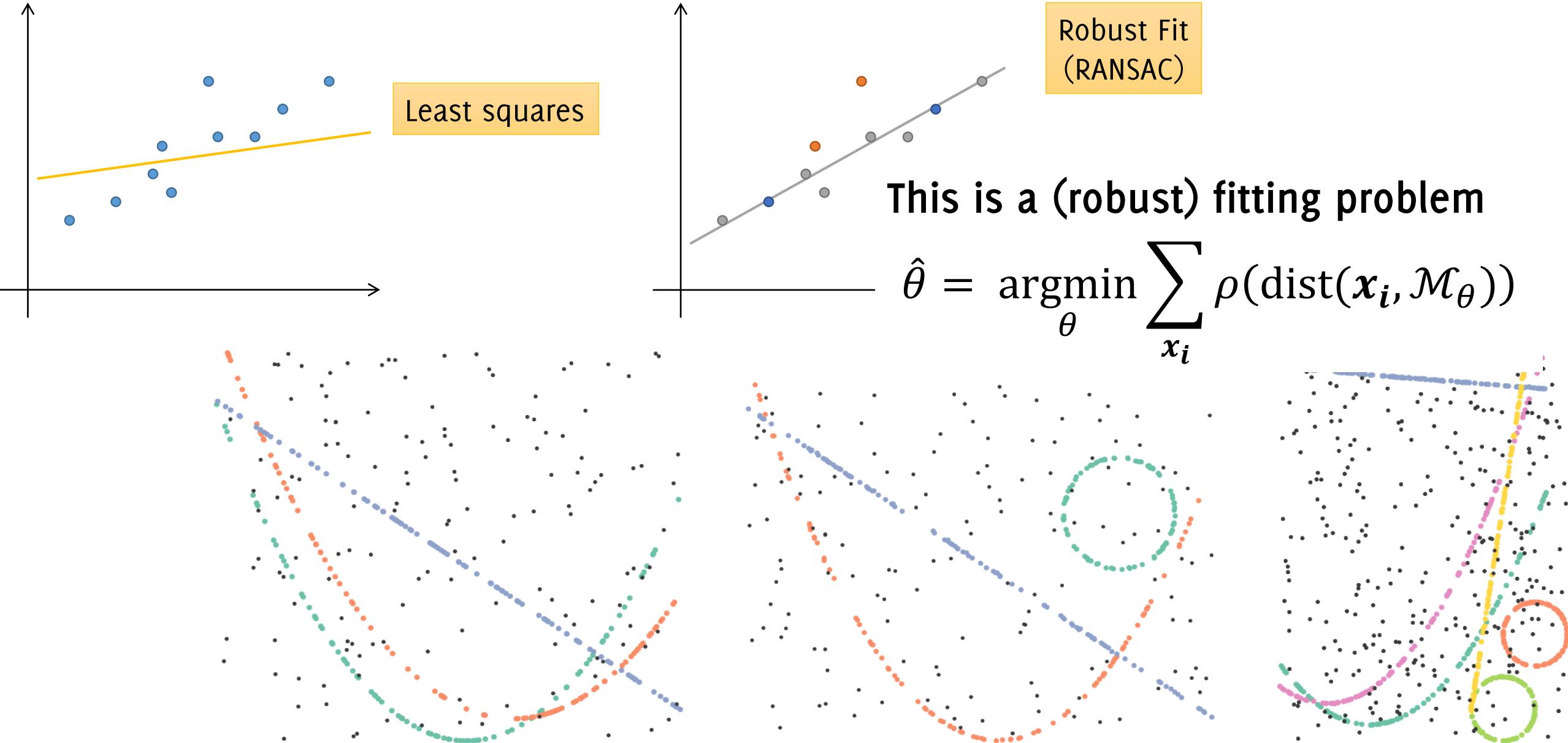
This boils down to Outlier Detection!

$$\hat{\phi}_0(\hat{x}) \geq \Gamma$$

where

$$\hat{x} = \operatorname{argmin}_x \frac{1}{2} \|Dx - z\|_2^2 + \lambda \|x\|_1$$

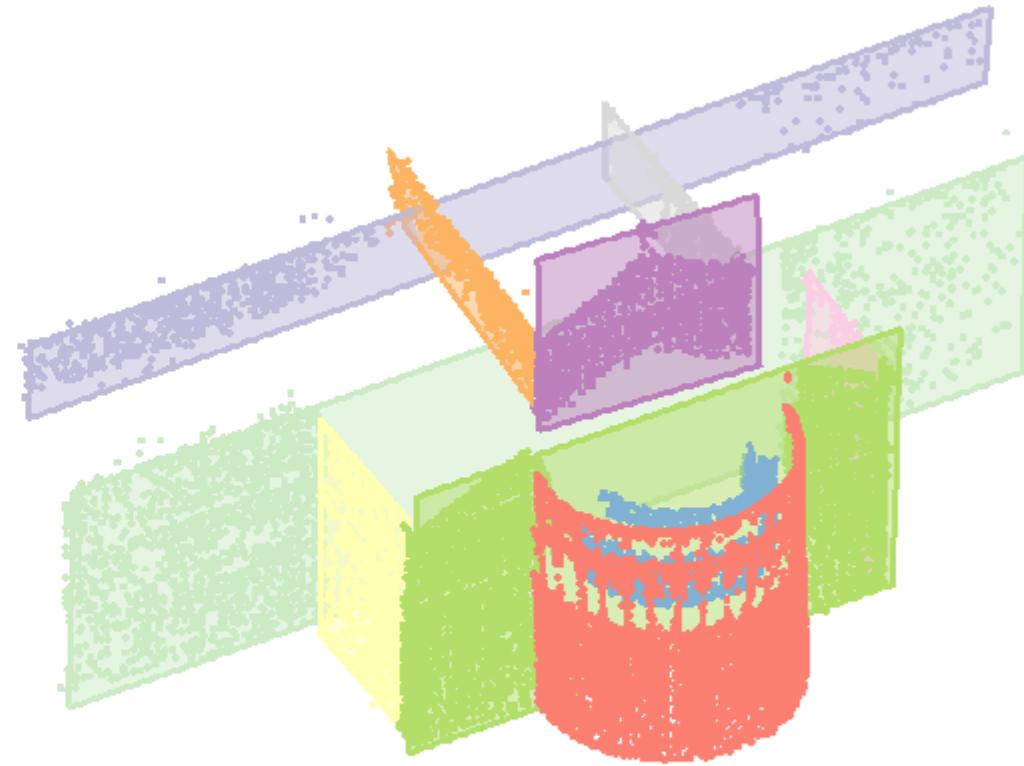
# Who cares about images? *visual recognition systems*



# Who cares about images? *visual recognition systems*



(a) Input point cloud



(b) Recovered structures

This is a (robust) fitting problem

# Who cares about images? visual recognition systems

12:30 Mar 19 mar

36% 



# Who cares about images? visual recognition systems

12:30 Mar 19 mar

36%



This is a (robust) fitting problem

**Is this interesting for a (perspective) Mathematical  
Engineer?**

# Is this interesting? Sure!

All the algorithms build upon:

- a clear problem formulation
- a simple mathematical model (...often linear combinations!)
- Sound mathematical solutions (linear algebra, least squares, convex optimization)

...and the result is not just a number... it's an image!

0k, to recap

# Mathematical Models and Methods for Image Processing (5 CFU)

*The primary goal of this laboratory course is to let the students design, implement and practice algorithms based on simple mathematical models from linear algebra and convex optimization, and solve challenging inverse problems in image processing (denoising, deblurring, inpainting, anomaly detection)*

# Mathematical Models and Methods for Image Processing (5 CFU)

The course topics include:

- **Image models based on orthonormal bases** (Fourier, wavelets), **data-driven basis** (PCA, Gram-Schmidt) and **local polynomial approximation**.
- **Sparsity and redundancy.**
  - Away from Orthonormal Basis, redundant set of generators
  - Sparse coding with  $\ell^0$  (OMP) or  $\ell^1$  norm (convex optimization ISTA, IRLS, LASSO)
  - Dictionaries yielding sparse representations and dictionary learning (KSVD)
- **Applications of sparse models** to image denoising, inpainting, anomaly detection and classification.
- **Robust fitting methods** (RANSAC, LMEDS, HOUGH) and their sequential counterparts for object detection in images.

# Course Organization

Lectures: 20 hours

Laboratory: 30 hours

There will be short theory recap and then you will be invited to develop and practice presented algorithms. Some demo code to fill in will be provided.

Simple assignment provided during lectures, oral exam.

# Frequently Asked Questions

**Q: Any specific background?**

*A: linear algebra, statistics and calculus*

**Q: Any programming skill required?**

*A: Proficiency in Matlab or Python*

**Q: Plenty of neural networks then?**

*A: No way. No neural networks allowed here\** ☺

*Only expert-driven algorithms designed upon a clear mathematical modeling that admits closed-form solutions / sound optimization schemes.*

# Questions?

Denoising over adaptively defined neighborhoods  
for local polynomial regression



## A few project and thesis opportunities

Updated thesis opportunities and furthre information on  
<https://boracchi.faculty.polimi.it/teaching.html>

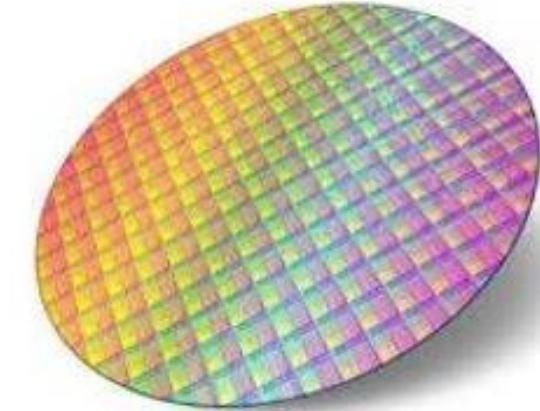
# Wafer Defect Maps Monitoring

Semiconductor manufacturing is a **long, complex and expensive** process involving several specialized steps

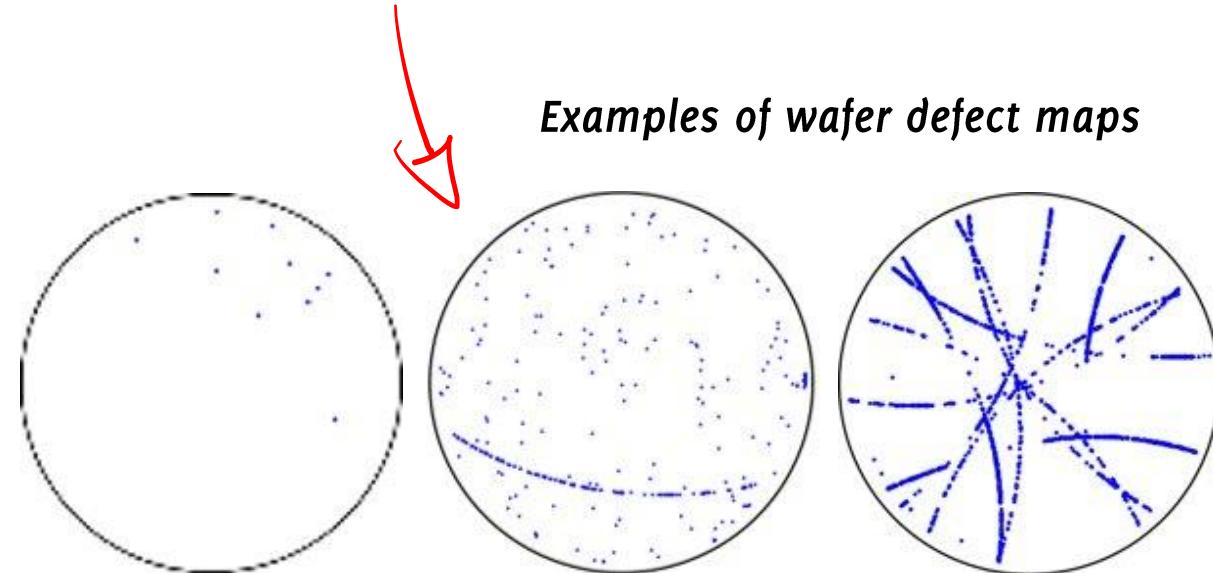
Inspection tools provide a **huge amount of data**, that can be entirely analysed only by **Deep Learning** techniques

Deep Learning enables the **automatic monitoring** of the production lines, **identifying defective patterns**. The results of this procedure allow to discard defective products and might promptly reveal failures of the machines

*A wafer containing multiple chips*



*Examples of wafer defect maps*



# Stage ST1: Wafer Defect Maps Monitoring

Currently, our automatic solution based on a CNN is classifying WDMs on the major production lines of STMicroelectronics site in Agrate. Future research will address

- The study of **domain adaptation** techniques to handle data coming from different production processes
- Design a solution to **identify the type of malfunctioning** and localize the faulty machinery in the production pipeline (metric learning)
- The development of an **anomaly-detection network** to identify never seen defective patterns

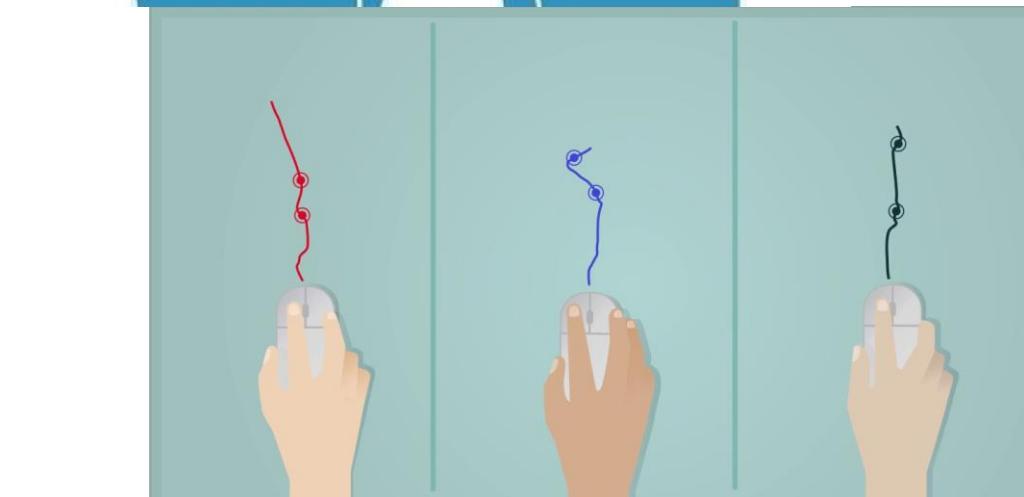
## Materials and methods:

- Annotated WDM dataset
- Support from ST's engineers
- Reference algorithm based on sparse convolutions

# Behavioral biometrics

**Behavioral biometrics** is the study related to uniquely identifiable and measurable patterns in human activities.

Behavioral biometric verification methods include **keystroke dynamics**, gait analysis, voice ID, mouse use characteristics, signature analysis and cognitive biometrics.



# Behavioral biometrics for fraud detection



- Discriminate between **humans** and **bots** (prevent **automated attacks**).
- Identify **fraudsters** (previously seen **malicious behaviors**).
- Predict the **credentials** through which the user will authenticate himself (likelihood of being a **specific known user**).
- Corroborate the identity of an **authenticated user**.

# Thesis: User Identification

**Goal:** Design and prototype an algorithm able to **verify** the user **identity** through his **behavioral biometrics** during a navigation session.

- Getting familiar with **state-of-the-art** behavioral biometrics verification **methods**.
- Robustly **profile users** through the various aforementioned methods.
- Continuously (and frictionless) **verify** the users **identities** during sessions.

## Materials and Methods:

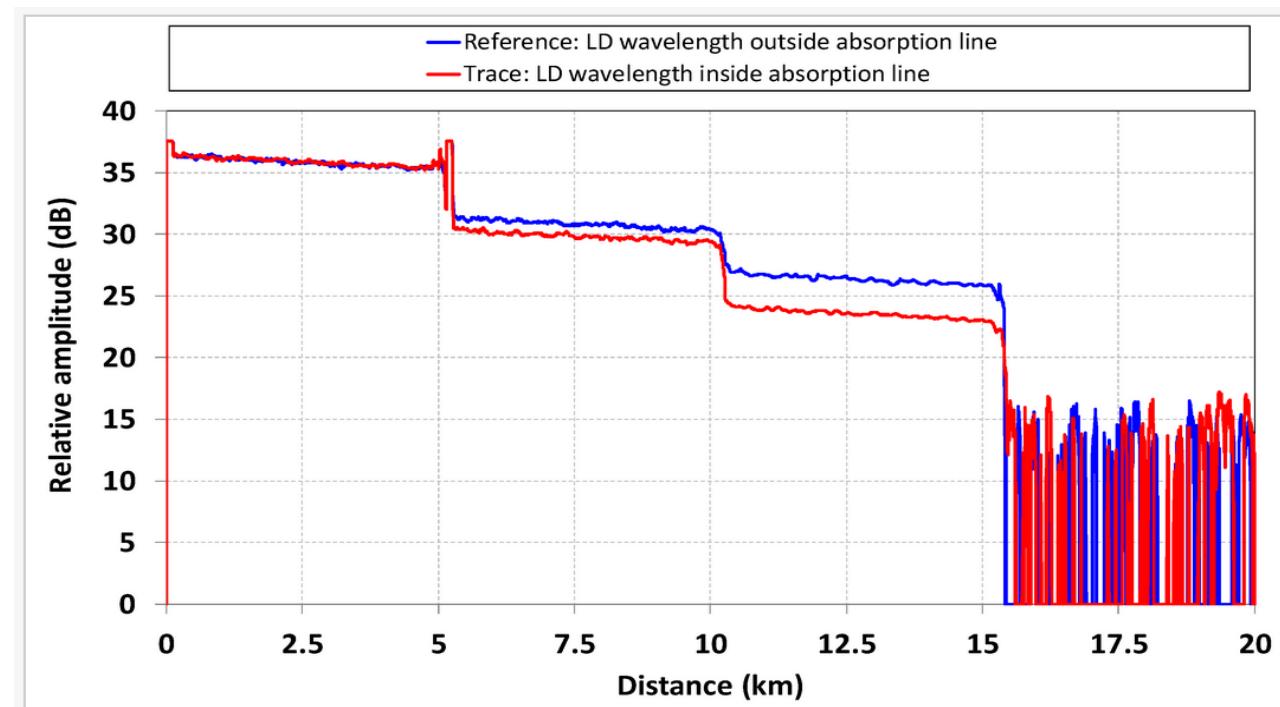
- Access to a server mounting GPUs will be provided.
- Anonymized data acquired from a large database of users.

Collaboration with  
Cleafy

# Stage CISCO: OTDR events recognition

OTDR (optical time domain reflectometer) is a technique to analyse a portion of an optical fiber.

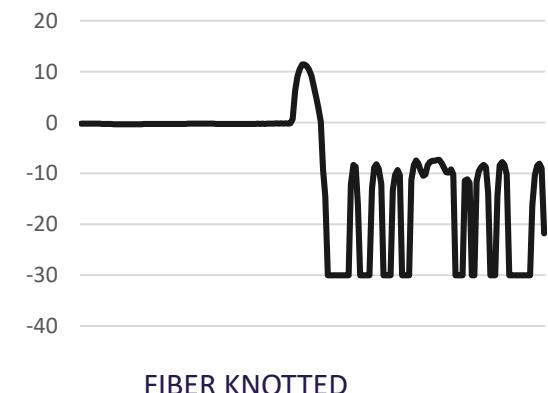
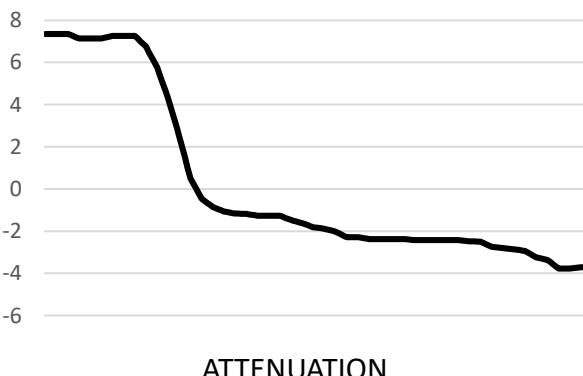
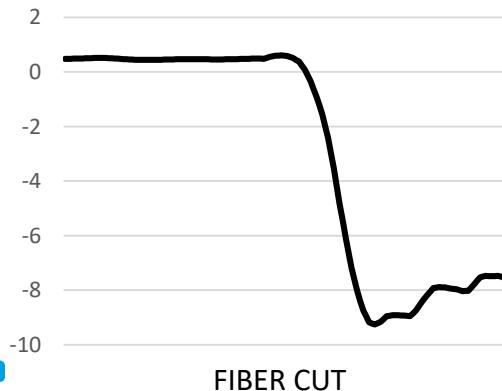
The output of OTDR is a signal representing the optical power (in dB) as a function of the distance (in Km) along the fiber.



# Stage CISCO: OTDR events recognition

Every span of optical fiber in the field features its own characteristic. OTDR signal has the potential to identify whether some event has occurred in the fiber span.

In practice, by analyzing OTDR signal it is possible to identify at which location in the fiber there has been a cut, a strong attenuation, the presence of reflection sources, or concentrated losses, to name a few examples:



# Stage CISCO: OTDR events recognition

## Goals:

- Implement a deep learning model to detect (multiple) patterns inside an OTDR signal. The model has to be 1-dimensional and able to cope with input signals of different dimensions.
- Define realistic data augmentation procedures in collaboration with CISCO engineers and scientists.
- Data set manipulation and preparation.
- Comparison among different solutions (expert-driven vs data-driven)
- Porting the final model on a real embedded systems.

## Materials and Methods:

- OTDR measurements from real fiber deployed in multiple sites.
- CISCO engineers will provide all the guidance and equipments needed.



# **A Laboratory Course (but not on deep learning)**

Next year, second semester (hopefully)

If you are planning to be here in a year...

*Laboratory of Mathematical Models and Techniques for Image and Signal Processing (5 CFU)*

Spring AA 2021 – 2022, Laboratory under preparation for Mathematical Engineers (and hopefully Computer Science Engineers)

*The course presents mathematical models underpinning several successful image/signal processing and pattern recognition algorithms, including the solution of inverse problems and fitting in noisy data. Particular emphasis will be given to models describing images as elements of a vector space, and the implications of linear algebra theory in imaging. These include transformed domain methods and other techniques to solve inverse problems.*

# Restoration & Inverse Problems



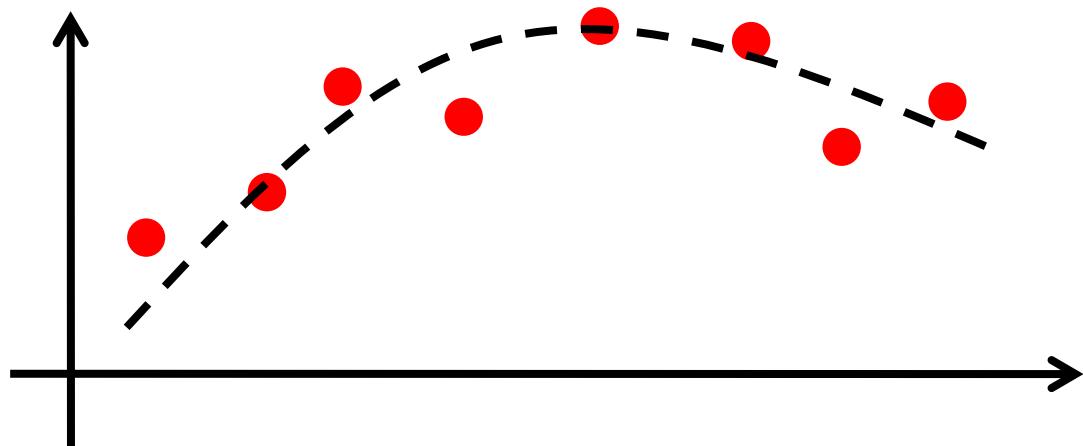
Dabov, K., Foi, A., Katkovnik, V., & Egiazarian, K. Image denoising by sparse 3-D transform-domain collaborative filtering. *TIP 2007*

# Restoration & Inverse Problems

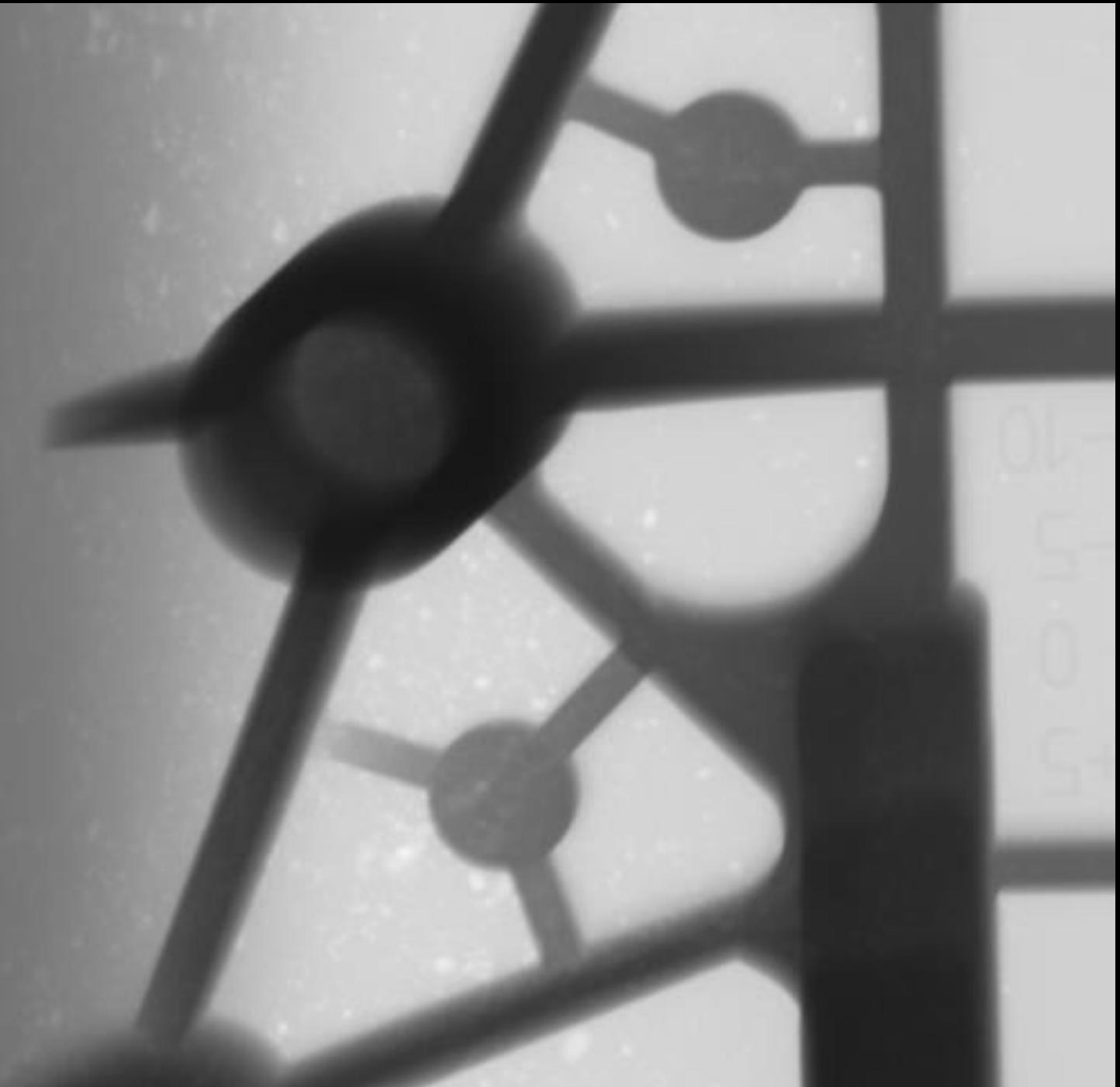


Dabov, K., Foi, A., Katkovnik, V., & Egiazarian, K. Image denoising by sparse 3-D transform-domain collaborative filtering. *TIP 2007*

# Filtering

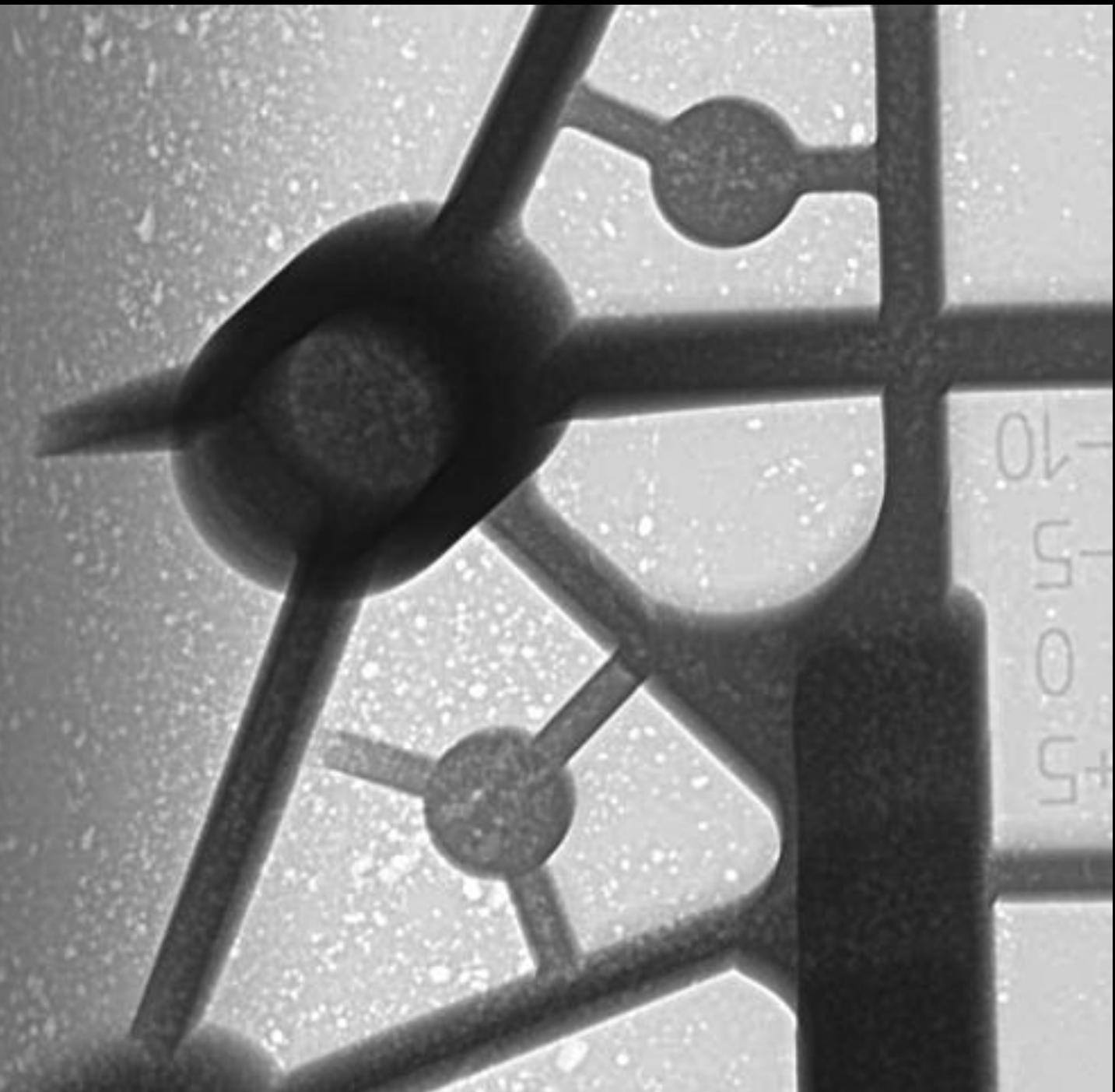


Input

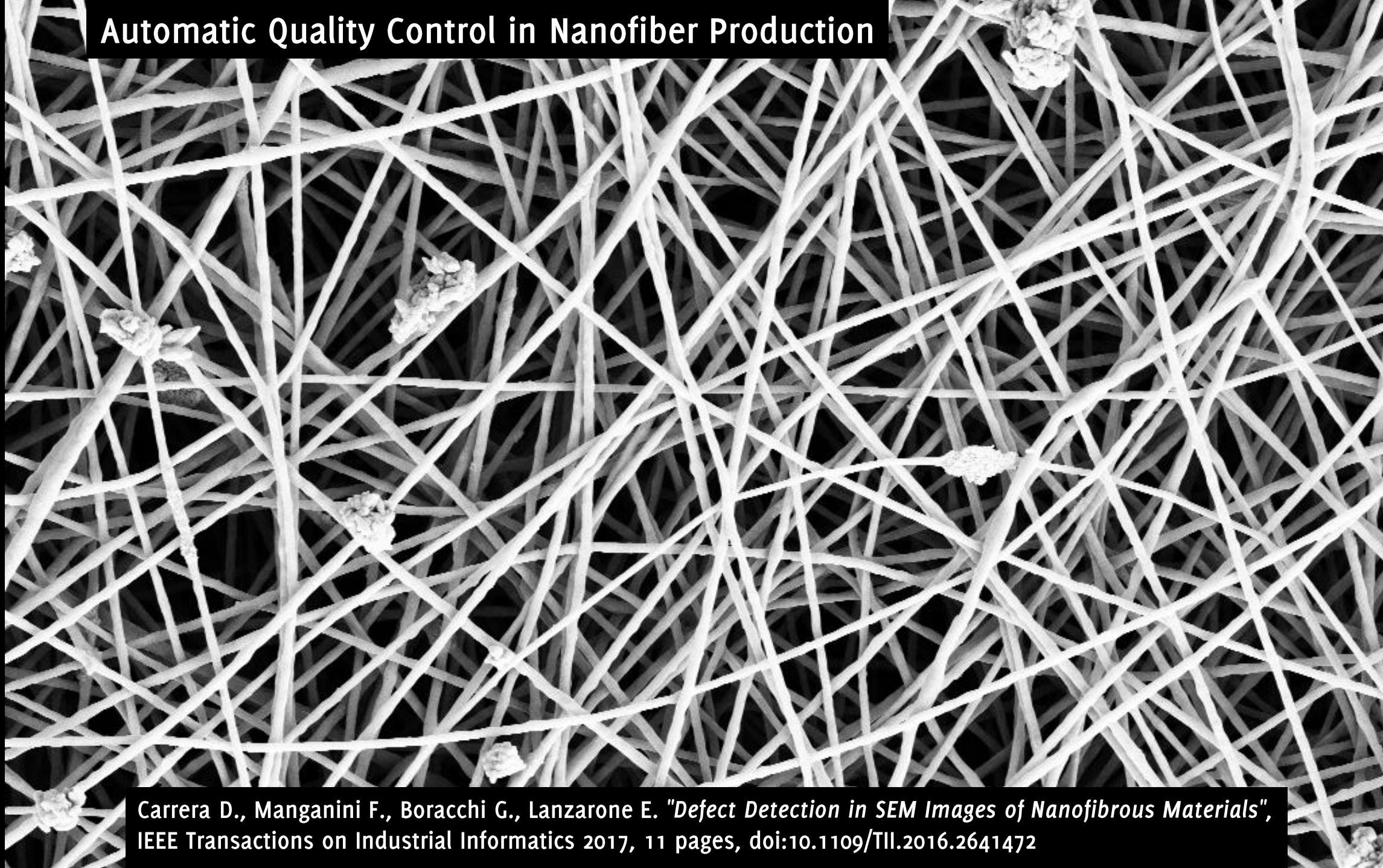


G. Boracchi

Enhanced



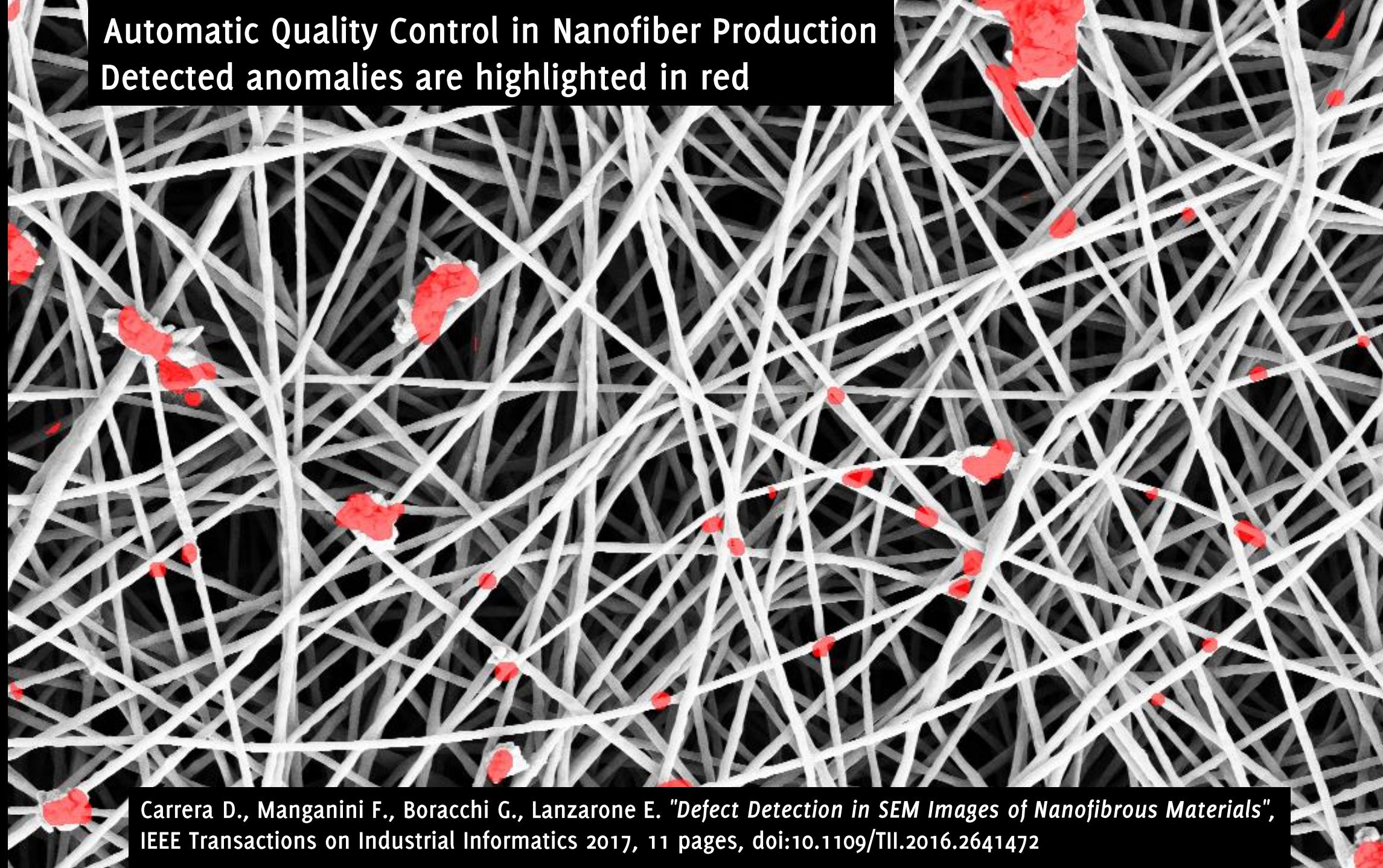
# Automatic Quality Control in Nanofiber Production



Carrera D., Manganini F., Boracchi G., Lanzarone E. "Defect Detection in SEM Images of Nanofibrous Materials", IEEE Transactions on Industrial Informatics 2017, 11 pages, doi:10.1109/TII.2016.2641472

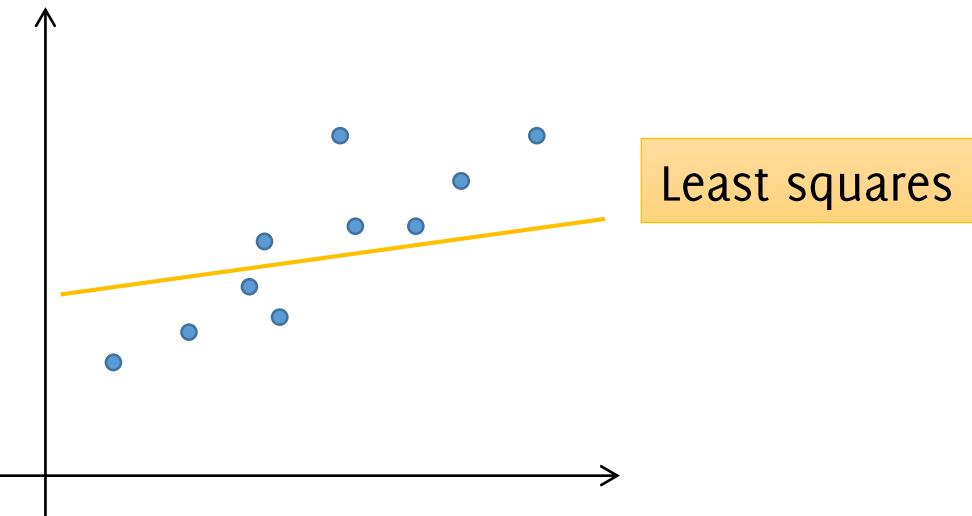
# Automatic Quality Control in Nanofiber Production

Detected anomalies are highlighted in red

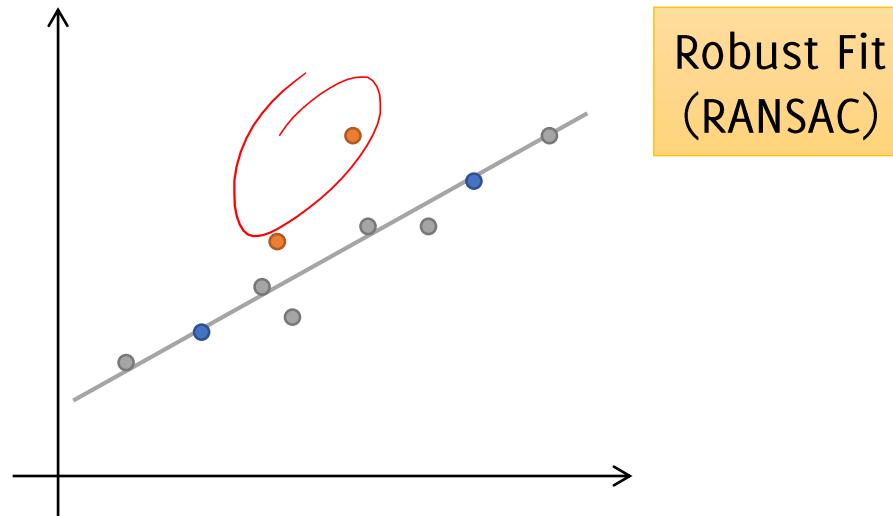


Carrera D., Manganini F., Boracchi G., Lanzarone E. "Defect Detection in SEM Images of Nanofibrous Materials", IEEE Transactions on Industrial Informatics 2017, 11 pages, doi:10.1109/TII.2016.2641472

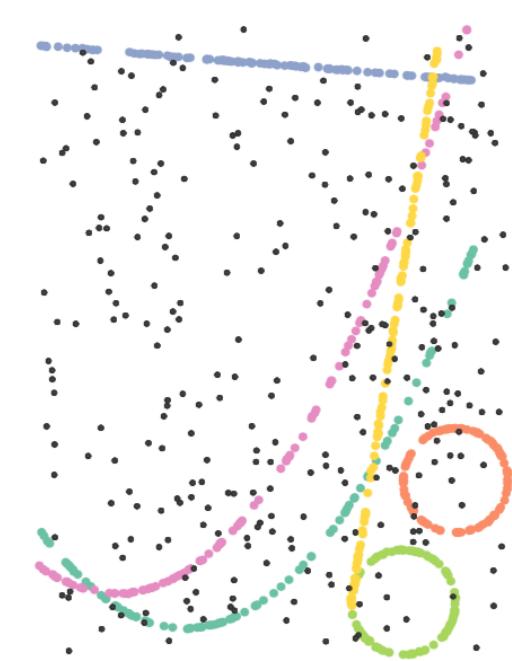
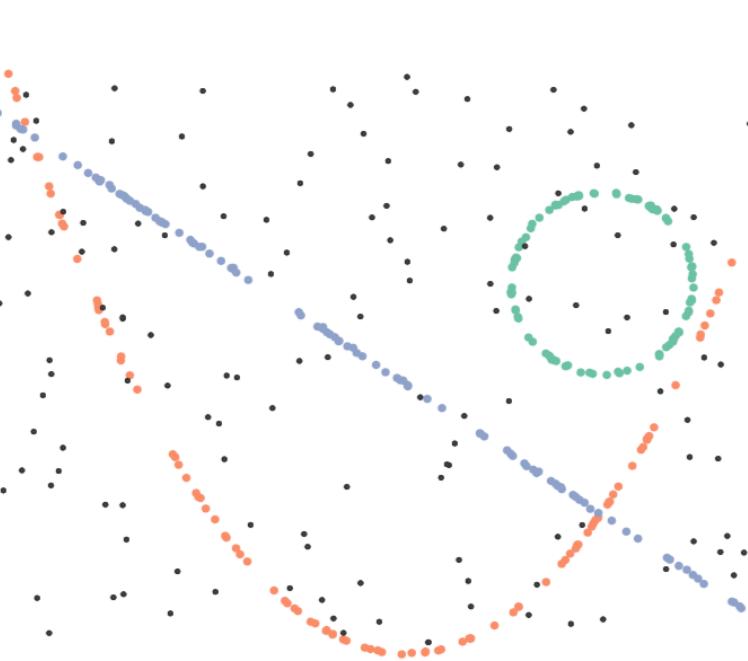
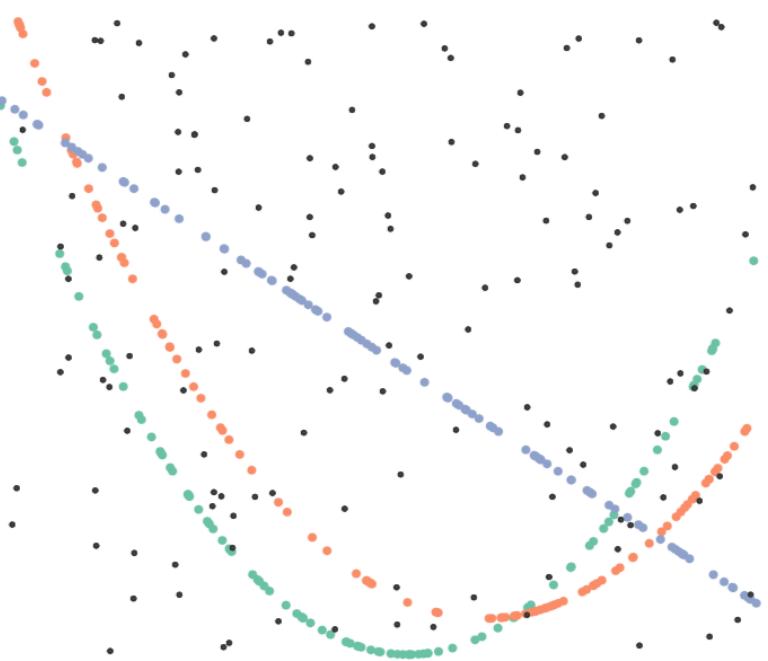
# Model Fitting



Least squares



Robust Fit  
(RANSAC)



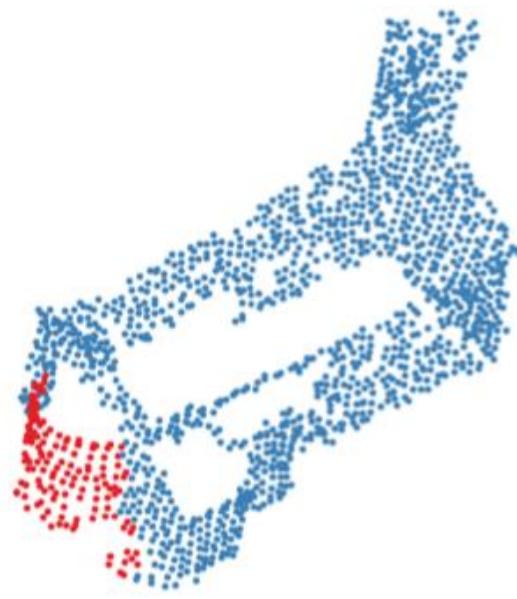
# Model Fitting



# Model Fitting



Image of the scene



colour coded class



colour coded model

Magri, Luca, and Andrea Fusiello. "Fitting Multiple Heterogeneous Models by Multi-Class Cascaded T-Linkage." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2019.

# **Learning Sparse Representations for Image and Signal Modeling**

a PhD Course open to MSc Students  
on February 2021

# A PhD Course open to MSc Students on February 2021

*The main goal of this course is to provide the student with an understanding of the most important aspects of the theory underlying sparse representation and, more in general, of sparsity as a form of regularization in learning problems. Students will have the opportunity to develop and understand the main algorithms for learning sparse models and computing sparse representations. These methods have wide applicability in computer science, and these will be a useful background for their research.*

*More information on the [Course program page](#)*

<https://boracchi.faculty.polimi.it/teaching/LearningSparse.htm>

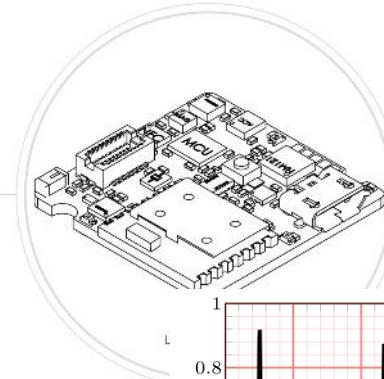
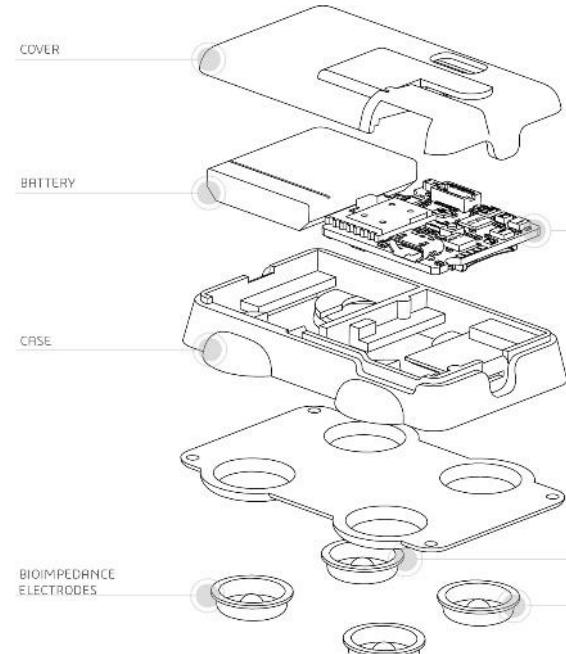
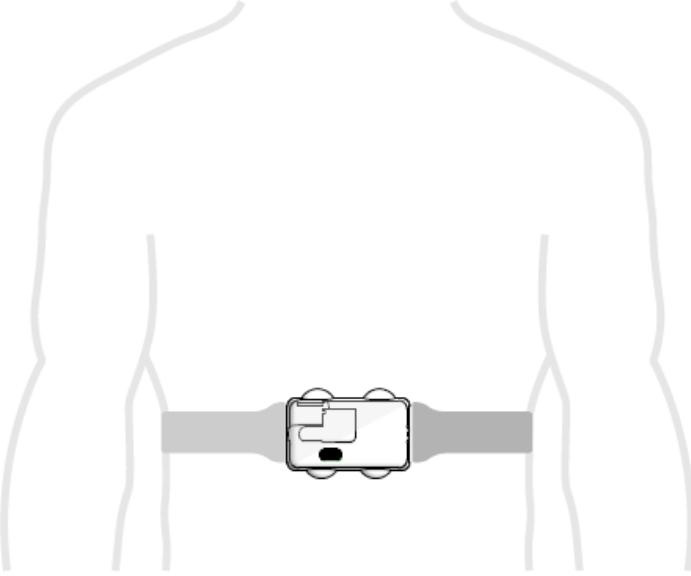
(dates to be updated)

# Dates

The course consists of traditional classes and computer-laboratory hours. During computer laboratory, students will be guided in the implementation of simplified versions of the presented algorithms. Imaging problems, including denoising, inpainting and anomaly detection, will be considered as running examples through the computer labs. Matlab is the preferred programming language (but you are of course allowed to use Python) and students are invited to work on their own laptop

- 02/02/2021 from 14:00 til 18:00
- 05/02/2021 from 14:00 til 19:00
- 09/02/2021 from 14:00 til 18:00
- 12/02/2021 from 14:00 til 18:00
- 16/02/2021 from 14:00 til 18:00
- 19/02/2021 from 14:00 til 18:00

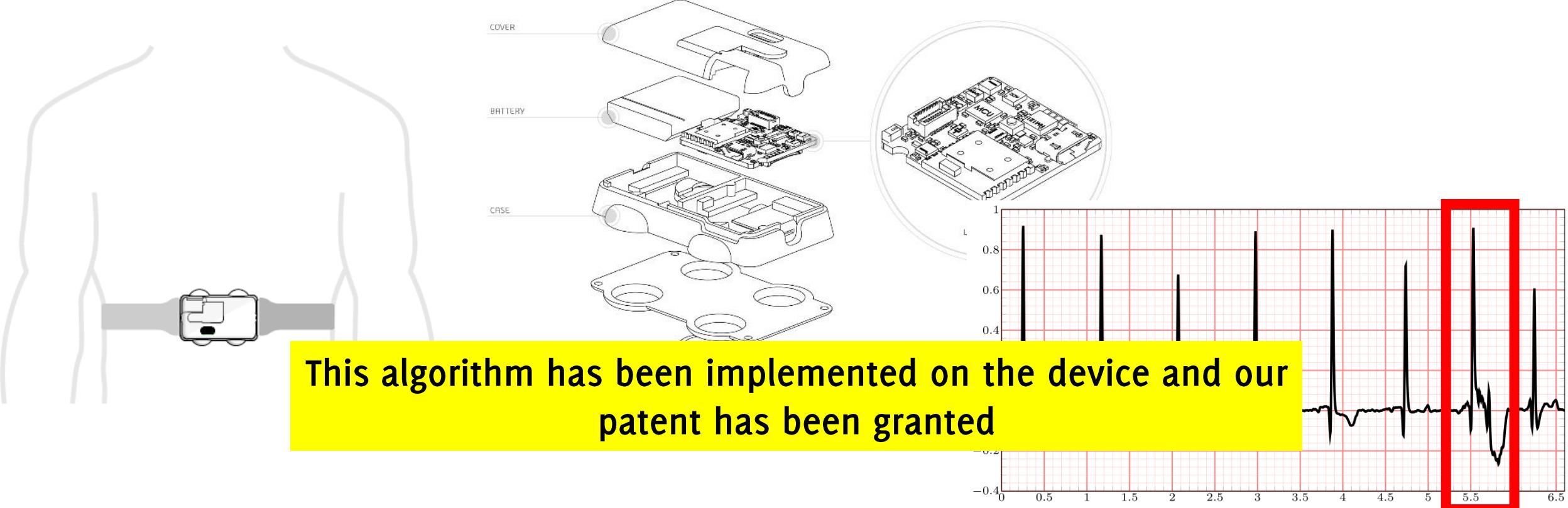
# An Example of algorithm we will see as an application: AD for Long Term ECG monitoring in wearables



A wearable device to enable **online and long term ECG monitoring**. Automatic **detection of anomalies** (e.g., arrhythmias) and **domain adaptation** to track heart rate variations. The model is based on a learned and user-specific model of heartbeats.

IJCAI Demo webpage: [http://home.deib.polimi.it/carrerad/IJCAI\\_2018\\_Demo.html](http://home.deib.polimi.it/carrerad/IJCAI_2018_Demo.html)

# An Example of algorithm we will see as an application: AD for Long Term ECG monitoring in wearables



This algorithm has been implemented on the device and our patent has been granted

A wearable device to enable **online and long term ECG monitoring**. Automatic **detection of anomalies** (e.g., arrhythmias) and **domain adaptation** to track heart rate variations. The model is based on a learned and user-specific model of heartbeats.

IJCAI Demo webpage: [http://home.deib.polimi.it/carrerad/IJCAI\\_2018\\_Demo.html](http://home.deib.polimi.it/carrerad/IJCAI_2018_Demo.html)