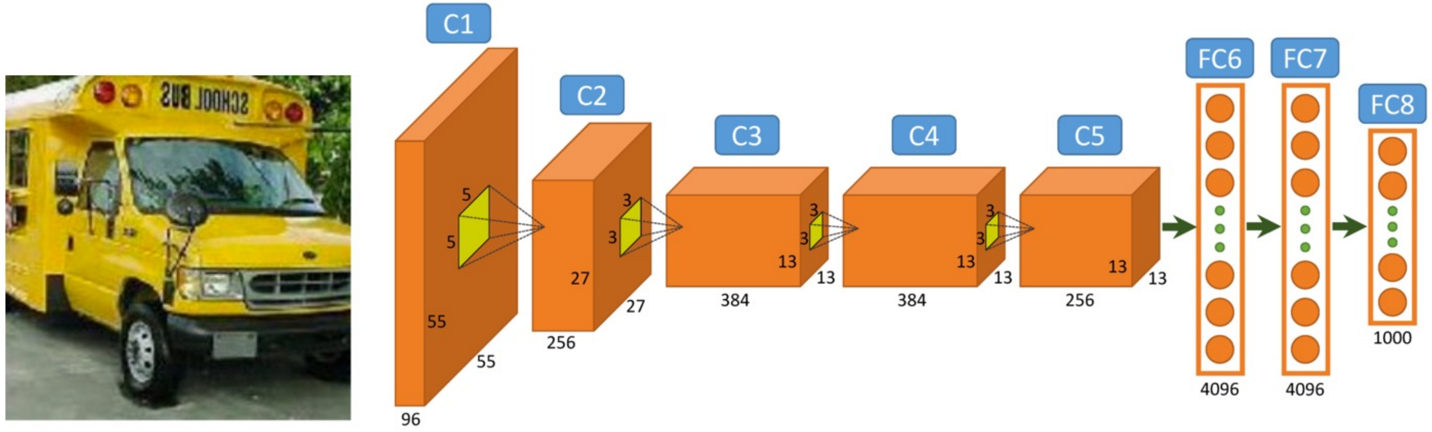
Deep Learning for Vision & Language

Feature-space Optimization: Adversarial Examples, GANs, Style Transfer

RICE UNIVERSITY

What we have been doing: Optimize weights in the network to predict bus (correct class).

I $\qquad\qquad y = f(I; w) \qquad\qquad L(y, bus)$

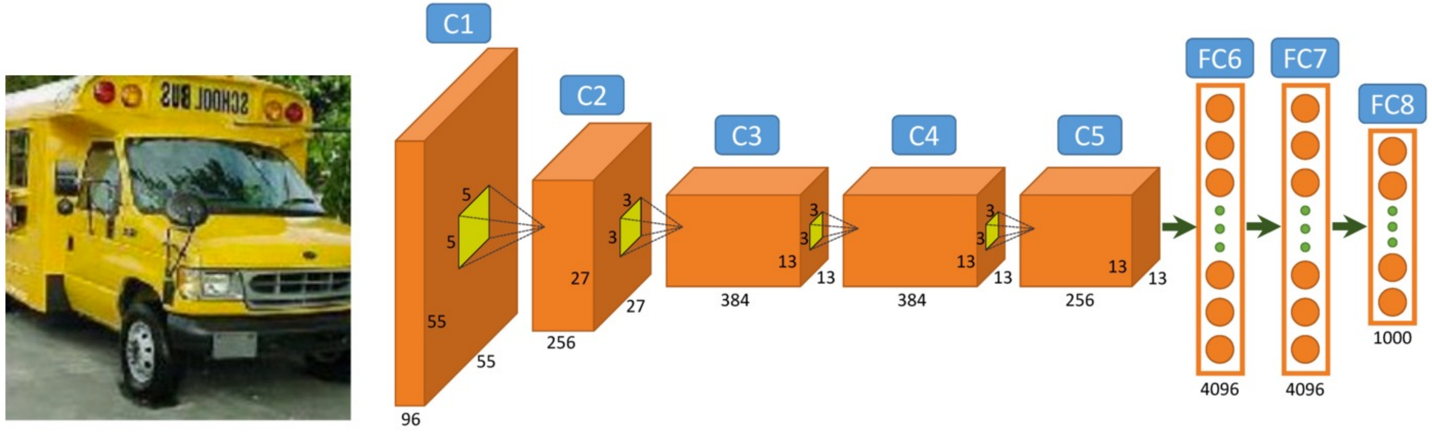


bus

$$w = w - \lambda \frac{\partial L}{\partial w}$$

New Idea: Create Adversarial Inputs by optimizing the input image to predict ostrich (wrong class).

I $\quad\quad$ $y = f(I; w)$ $\quad\quad$ $L(y, ostrich)$

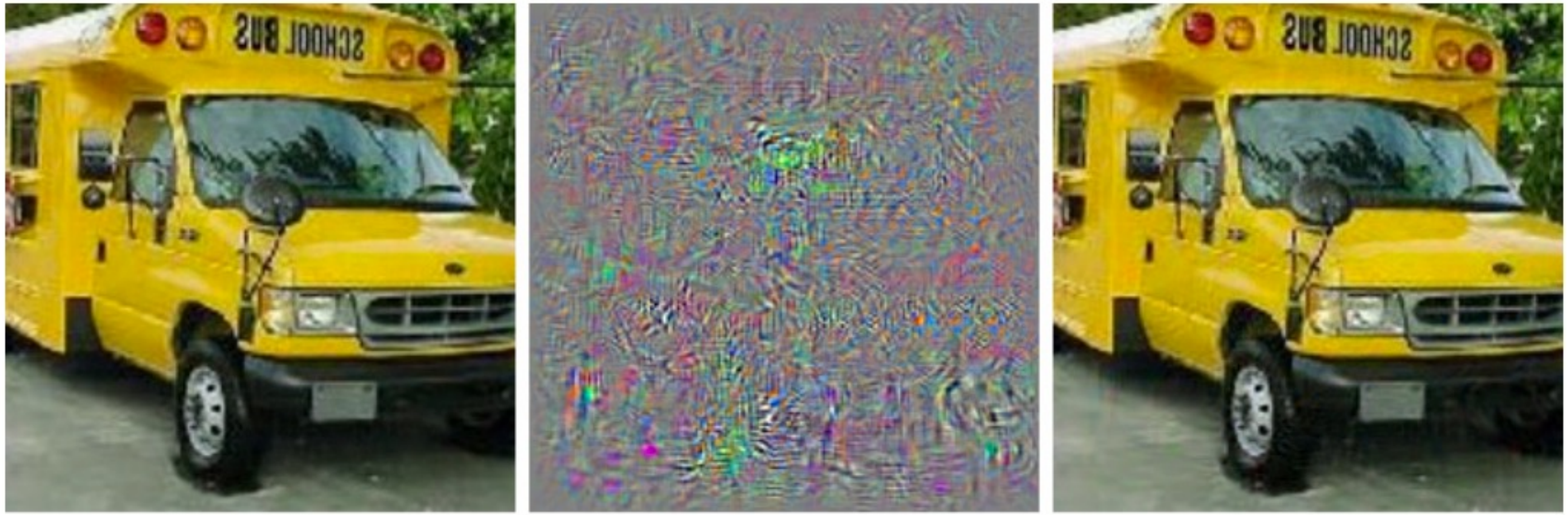


ostrich

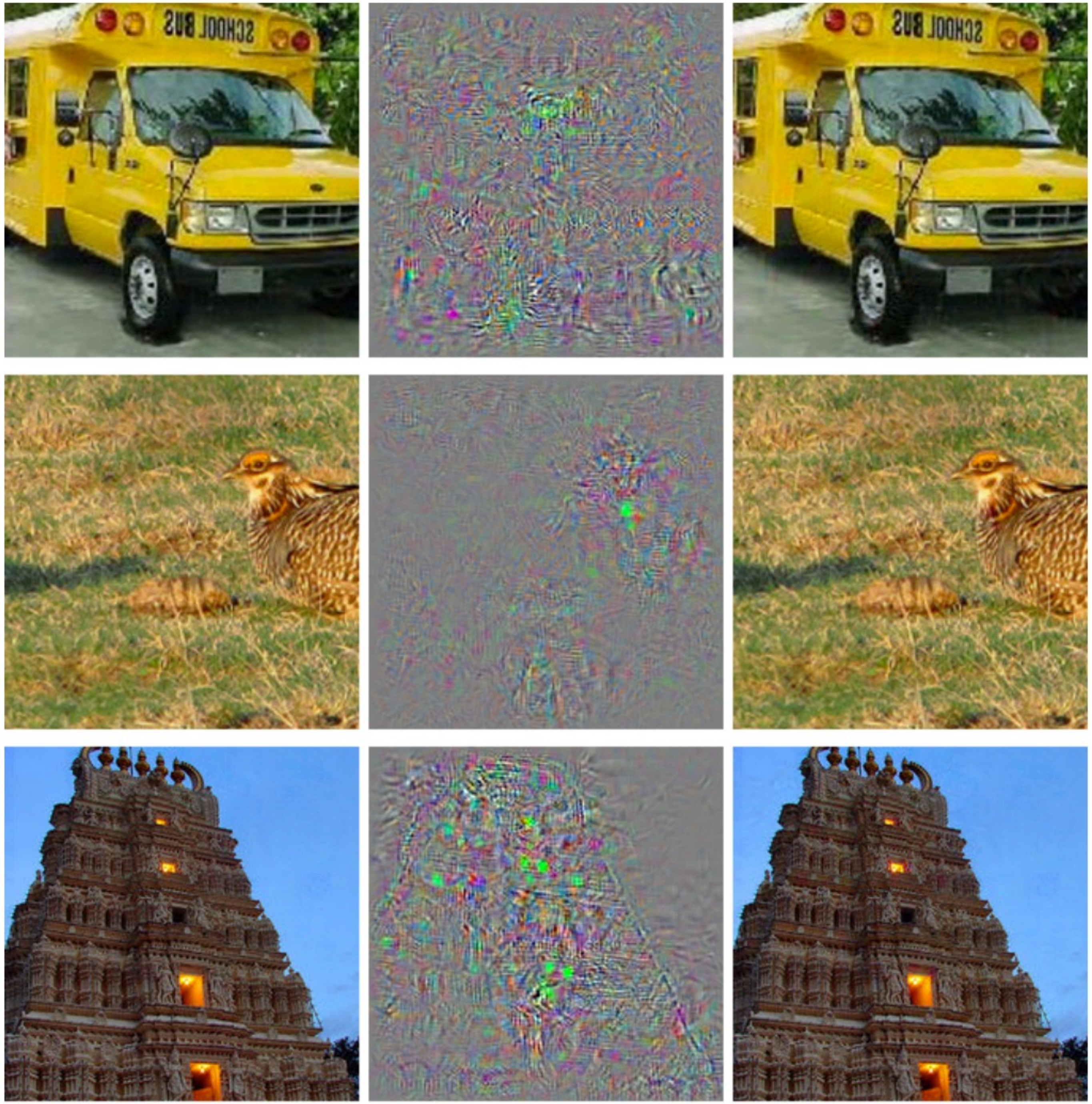
$$I = I - \lambda \frac{\partial L}{\partial I}$$

Work on Adversarial examples by Goodfellow et al. , Szegedy et. al., etc.

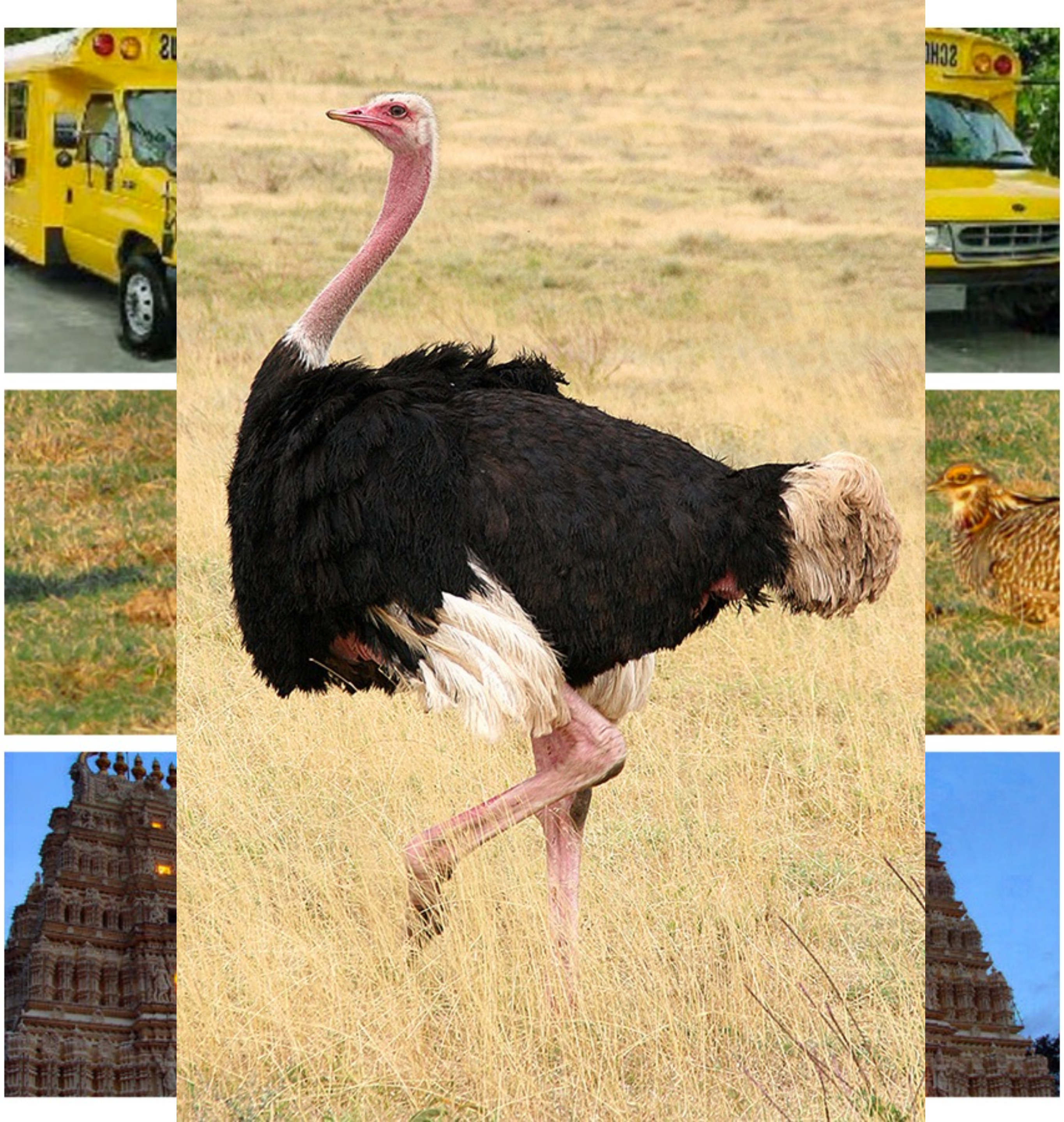
Convnets (optimize input to predict ostrich)



Work on Adversarial examples by Goodfellow et al. , Szegedy et. al., etc.



All get predicted as ostrich



Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

Anh Nguyen, Jason Yosinski, Jeff Clune, 2014

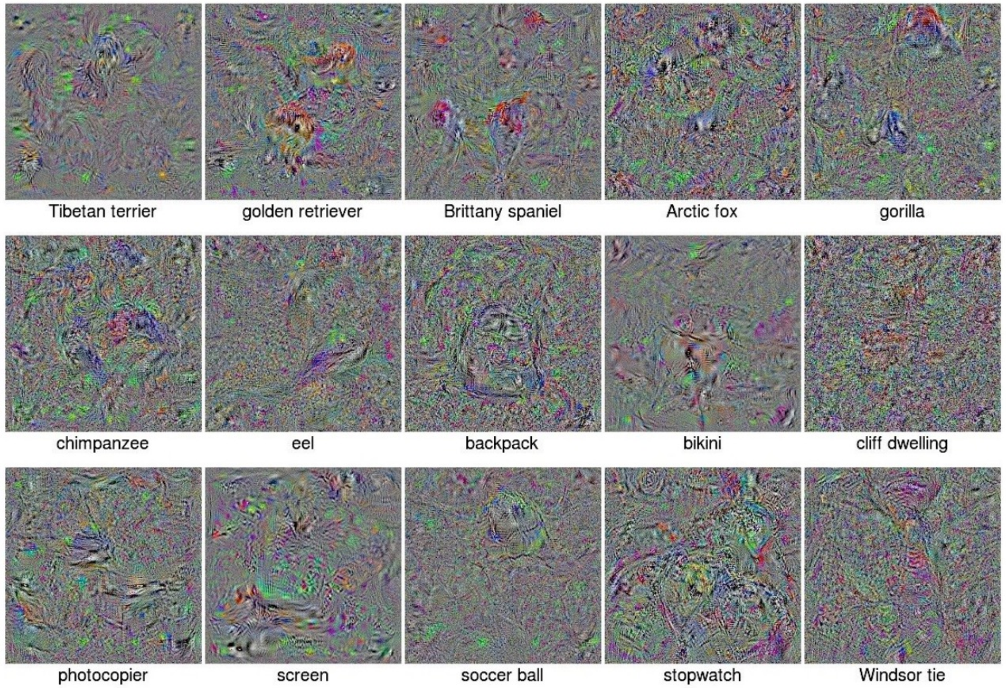
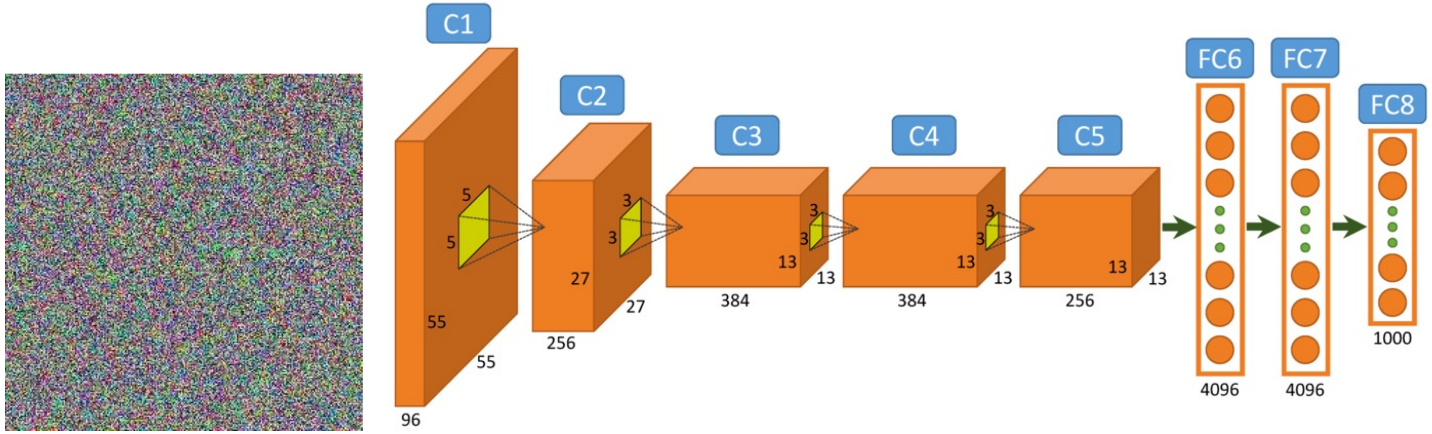


Figure 13. Images found by maximizing the softmax output for classes via gradient ascent [11, 26]. Optimization begins at the ImageNet mean (plus small Gaussian noise to break symmetry) and continues until the DNN confidence for the target class reaches 99.99%. Images are shown with the mean subtracted. Adding regularization makes images more recognizable but results in slightly lower confidence scores (see supplementary material).

New Idea: Create Adversarial Inputs by optimizing the input image to predict ostrich (wrong class).

I $\qquad y = f(I; w) \qquad L(y, parking\ meter)$



parking meter

$$I = I - \lambda \frac{\partial L}{\partial I}$$

Work on Adversarial examples by Goodfellow et al. , Szegedy et. al., etc.

parking meter: 0.999679

Total Variation Regularization

A second richer regulariser is *total variation* (TV) $\mathcal{R}_{V^\beta}(\mathbf{x})$, encouraging images to consist of piece-wise constant patches. For continuous functions (or distributions) $f : \mathbb{R}^{H \times W} \supset \Omega \to \mathbb{R}$, the TV norm is given by:

$$\mathcal{R}_{V^\beta}(f) = \int_\Omega \left(\left(\frac{\partial f}{\partial u}(u,v) \right)^2 + \left(\frac{\partial f}{\partial v}(u,v) \right)^2 \right)^{\frac{\beta}{2}} du\, dv$$

where $\beta = 1$. Here images are discrete ($\mathbf{x} \in \mathbb{R}^{H \times W}$) and the TV norm is replaced by the finite-difference approximation:

$$\mathcal{R}_{V^\beta}(\mathbf{x}) = \sum_{i,j} \left((x_{i,j+1} - x_{ij})^2 + (x_{i+1,j} - x_{ij})^2 \right)^{\frac{\beta}{2}}.$$

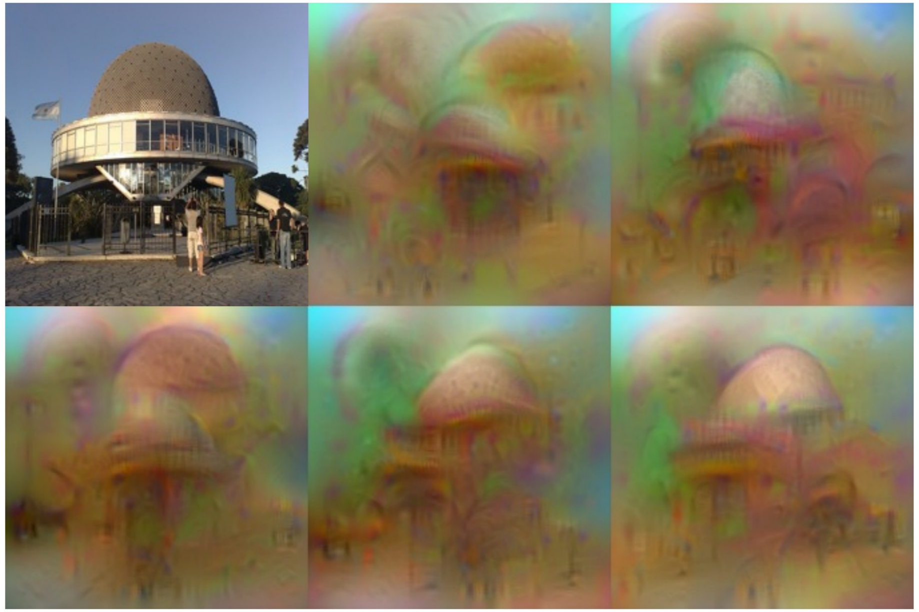
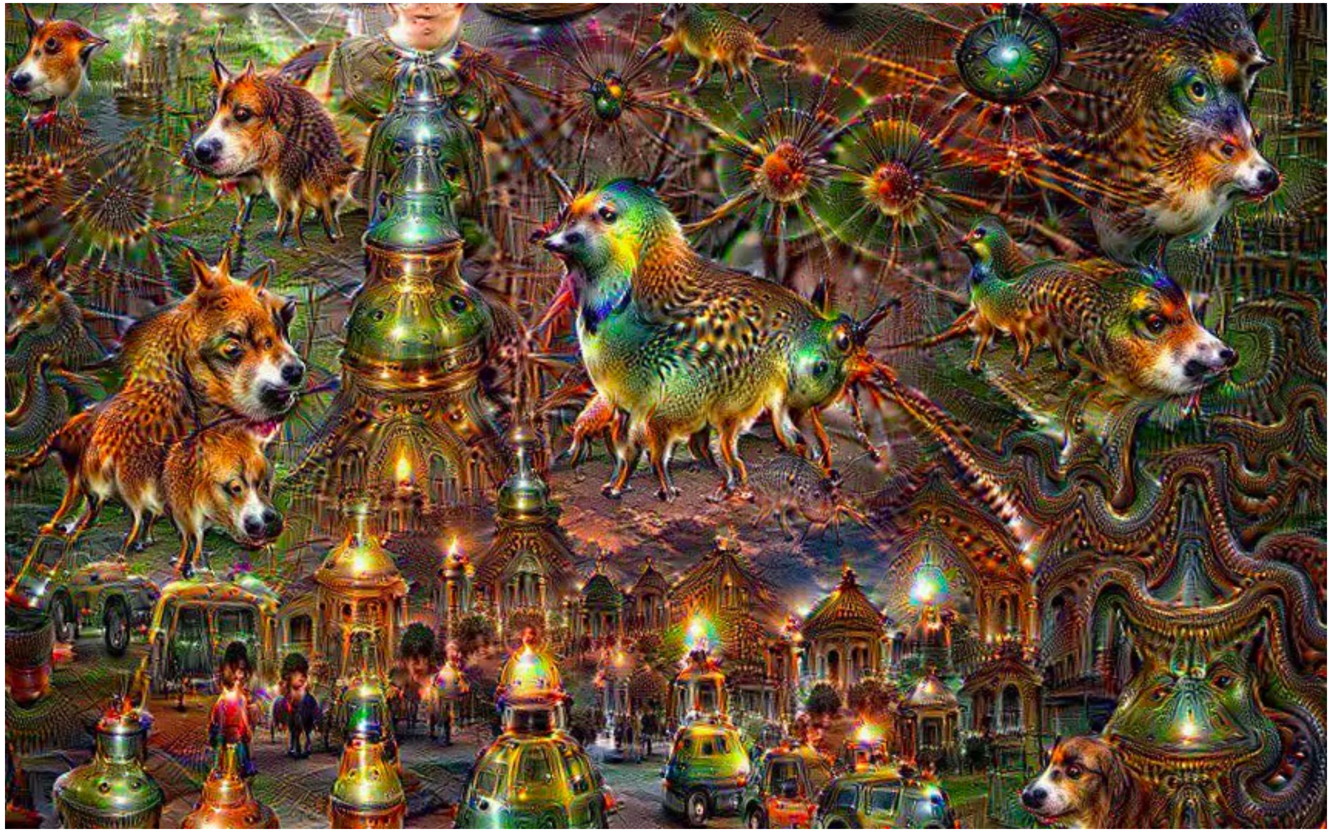


Figure 1. **What is encoded by a CNN?** The figure shows five possible reconstructions of the reference image obtained from the 1,000-dimensional code extracted at the penultimate layer of a reference CNN[13] (before the softmax is applied) trained on the ImageNet data. From the viewpoint of the model, all these images are practically equivalent. This image is best viewed in color/screen.

Mahendran and Vedaldi, Understanding Deep Image Representations by Inverting Them, 2014

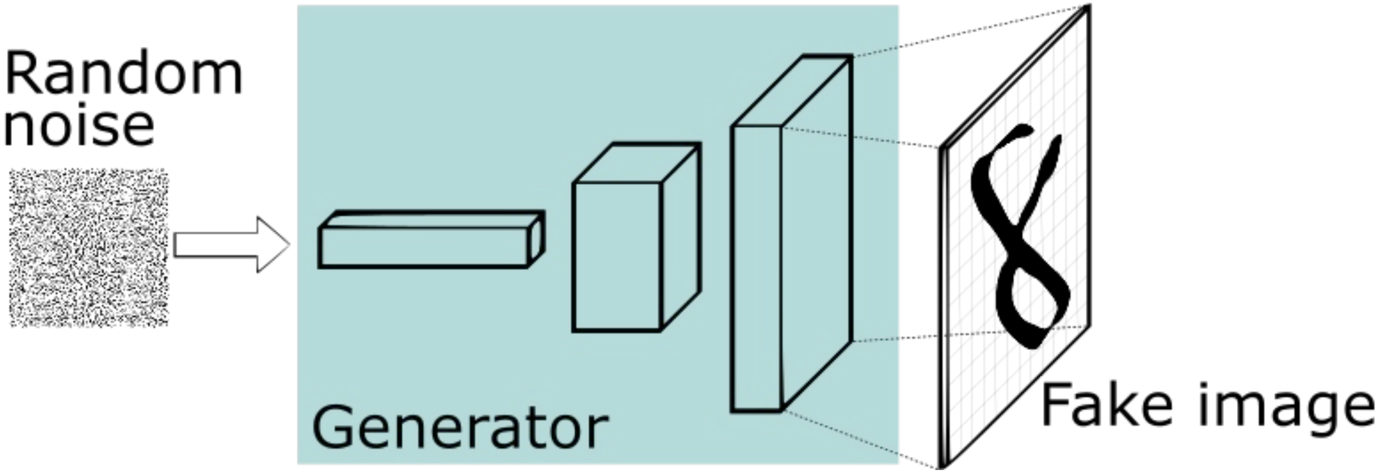
Taking the idea to the extreme: Google's DeepDream



https://research.googleblog.com/2015/06/inceptionism-going-deeper-into-neural.html

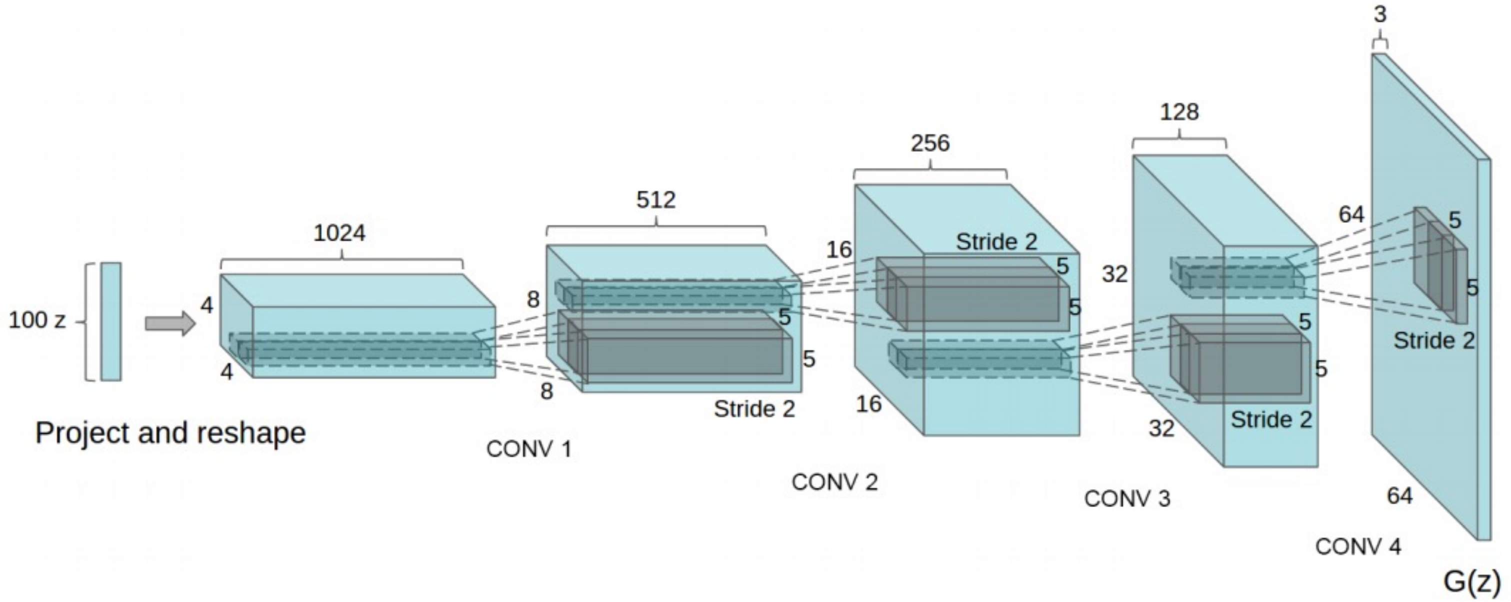
Generate your own in Pytorch: https://github.com/XavierLinNow/deepdream_pytorch

Generative Adversarial Networks (GAN) [Goodfellow et al 2014]



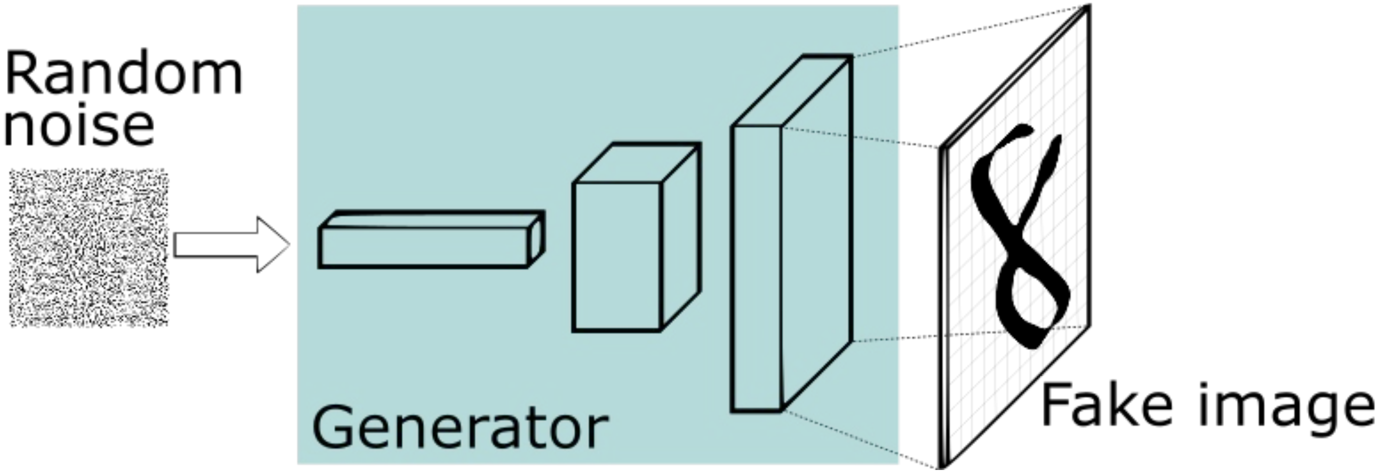
https://deeplearning4j.org/generative-adversarial-network

Generative Network (closer look)



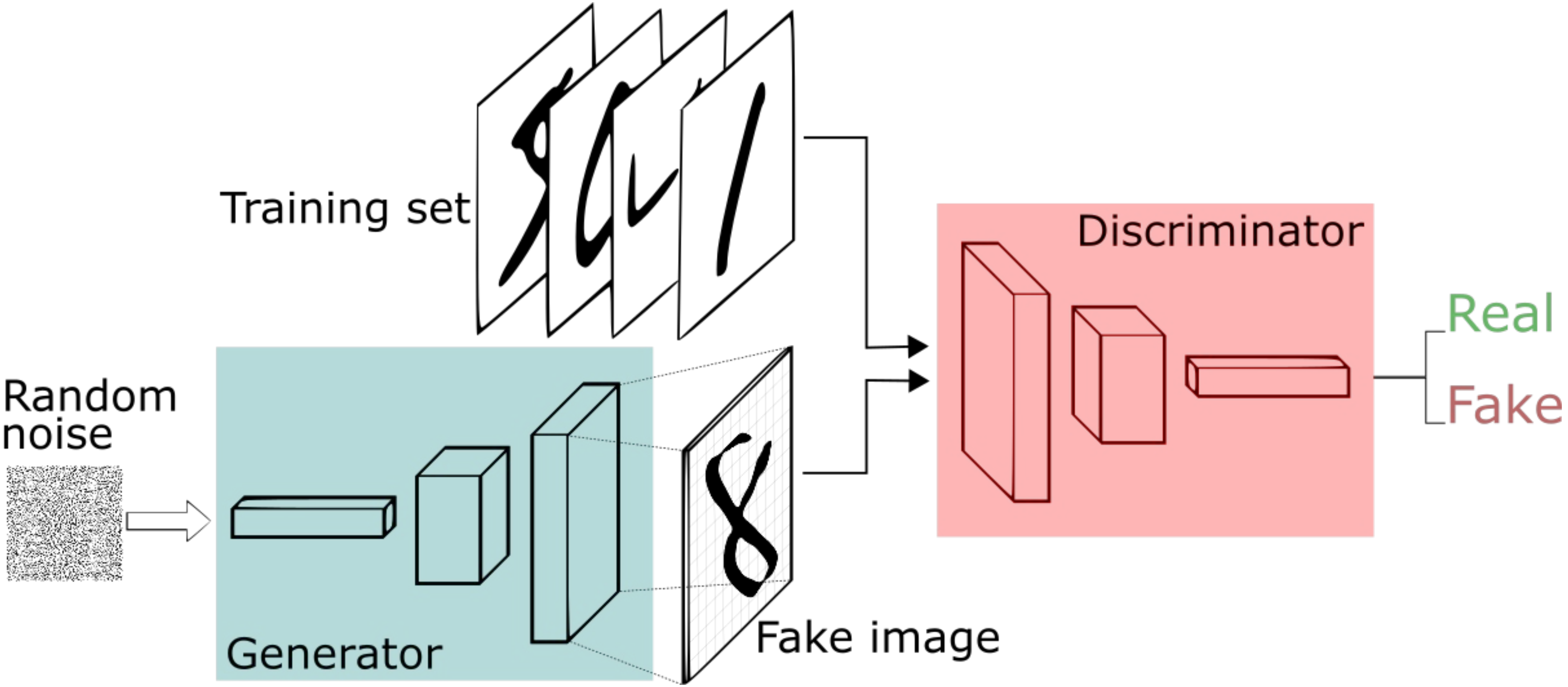
Radford et. al. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks. ICLR 2016

Generative Adversarial Networks (GAN) [Goodfellow et al.]



https://deeplearning4j.org/generative-adversarial-network

Generative Adversarial Networks (GAN) [Goodfellow et al.]



https://deeplearning4j.org/generative-adversarial-network

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

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

  end for

  - Sample minibatch of m noise samples $\{\boldsymbol{z}^{(1)}, \ldots, \boldsymbol{z}^{(m)}\}$ from noise prior $p_g(\boldsymbol{z})$.
  - Update the generator by descending its stochastic gradient:

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

end for

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

Goodfellow et al. NeurIPS 2014

Update Discriminator D

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

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

end for

- Sample minibatch of m noise samples $\{\boldsymbol{z}^{(1)}, \dots, \boldsymbol{z}^{(m)}\}$ from noise prior $p_g(\boldsymbol{z})$.
- Update the generator by descending its stochastic gradient:

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

end for

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

Goodfellow et al. NeurIPS 2014

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

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

  end for

Update Generator G

  - Sample minibatch of m noise samples $\{\boldsymbol{z}^{(1)}, \dots, \boldsymbol{z}^{(m)}\}$ from noise prior $p_g(\boldsymbol{z})$.
  - Update the generator by descending its stochastic gradient:

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

end for

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

Goodfellow et al. NeurIPS 2014

Until Desirable Results are Achieved?

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

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

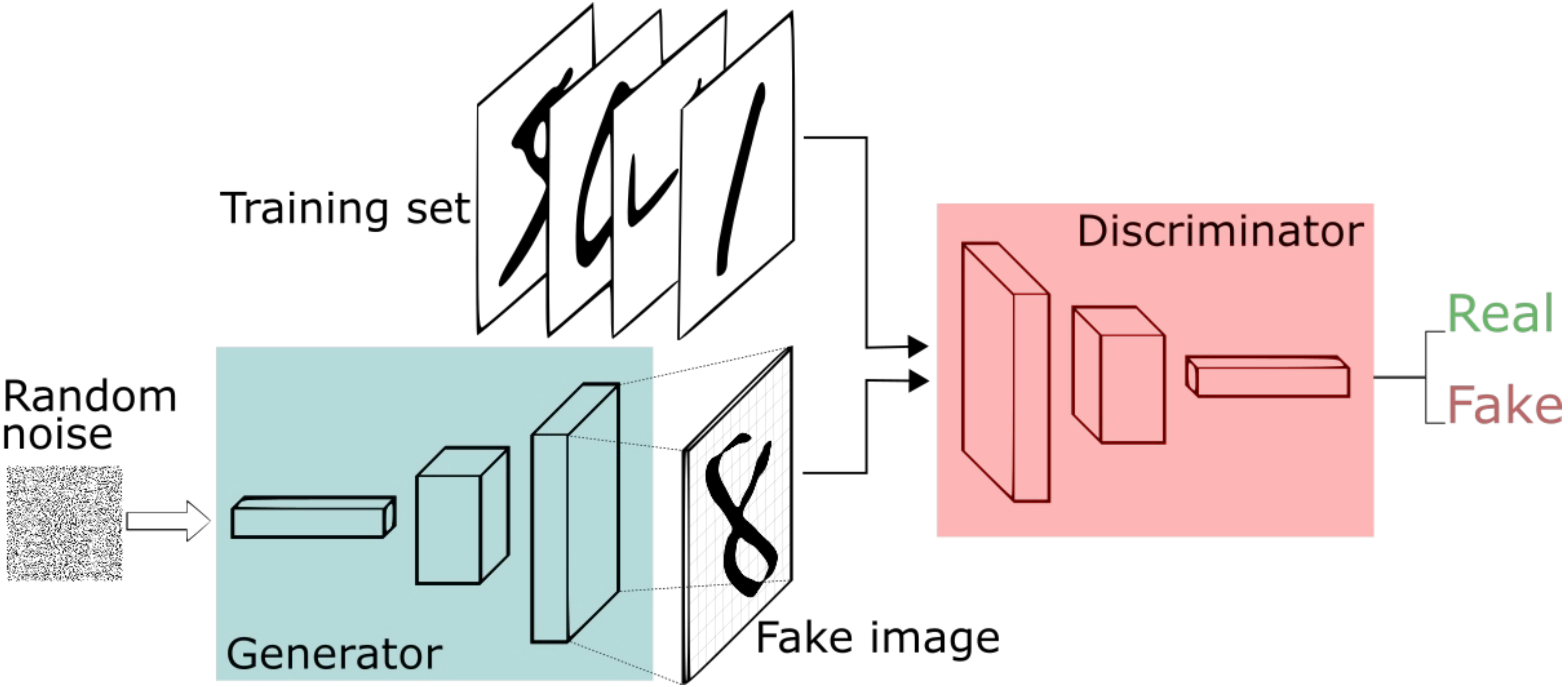
  end for
  - Sample minibatch of m noise samples $\{\boldsymbol{z}^{(1)}, \ldots, \boldsymbol{z}^{(m)}\}$ from noise prior $p_g(\boldsymbol{z})$.
  - Update the generator by descending its stochastic gradient:

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

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

Goodfellow et al. NeurIPS 2014

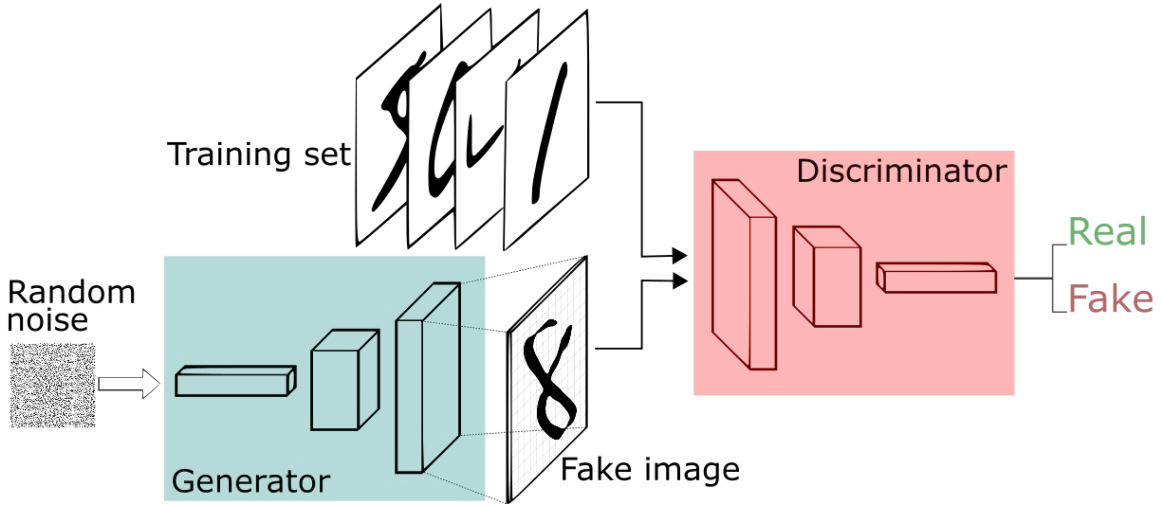
Generative Adversarial Networks (GAN) [Goodfellow et al.]



https://deeplearning4j.org/generative-adversarial-network

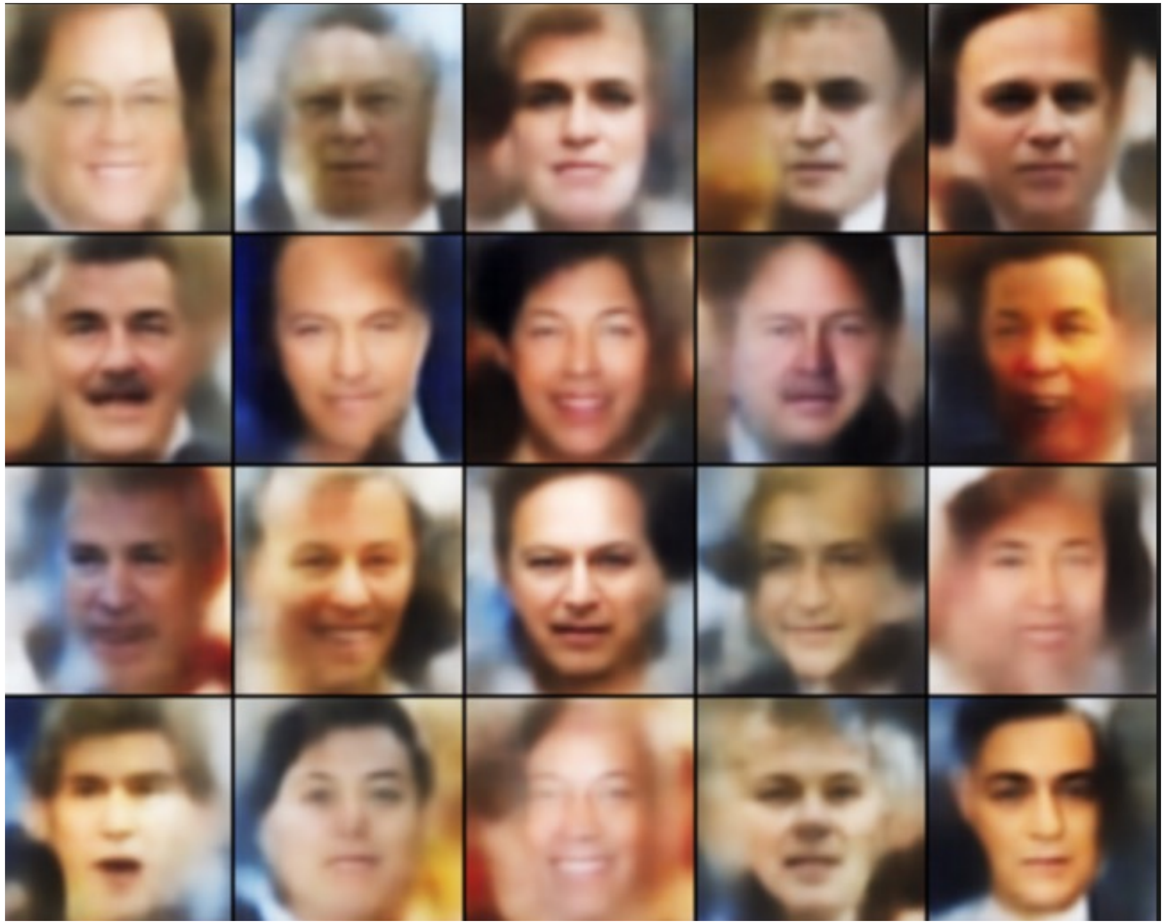
Generative Adversarial Networks (GAN) [Goodfellow et al.]

- GANs are hard to train, loss for the discriminator and generator might fluctuate.
- There are many choices for loss, and other auxiliary signals.
- Training of these models is even less well understood than for other deep models.



https://deeplearning4j.org/generative-adversarial-network

Basic GAN Results (Example implementation is provided in Pytorch's examples)



http://torch.ch/blog/2015/11/13/gan.html

NVidia's progressive GANs ICLR 2018

Google’s BigGAN

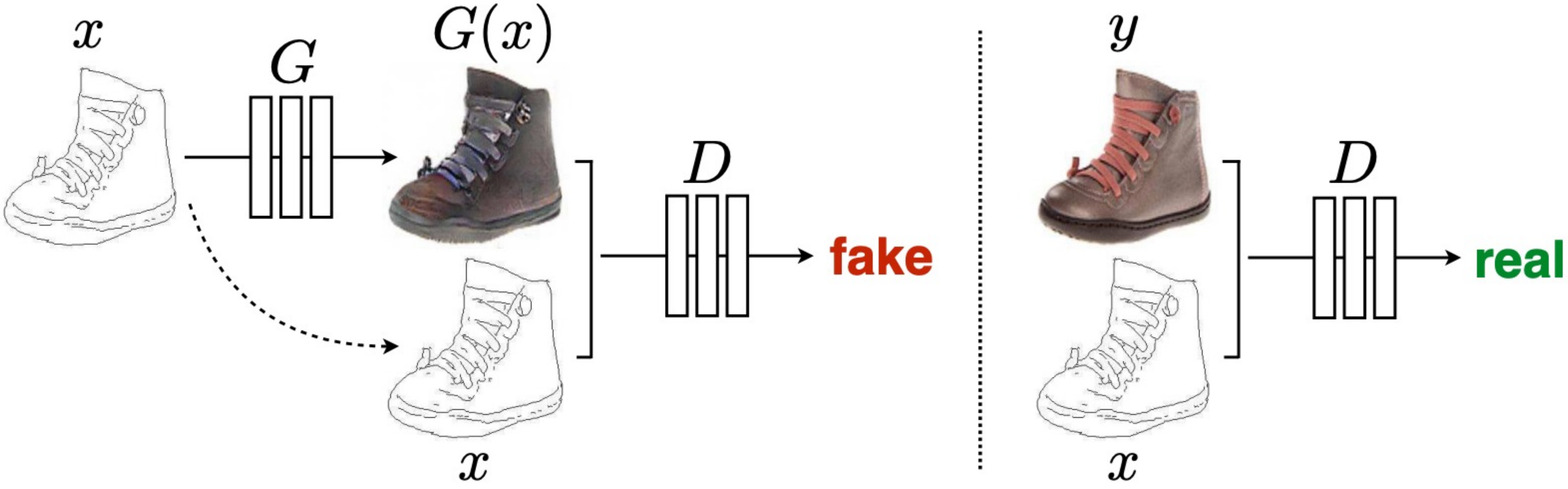
Google's BigGAN

Teddy Bear

Microphone

http://aiweirdness.com/post/179626595787/the-creepiest-images-generated-by-biggan

Conditional GANs: Input is not just Noise

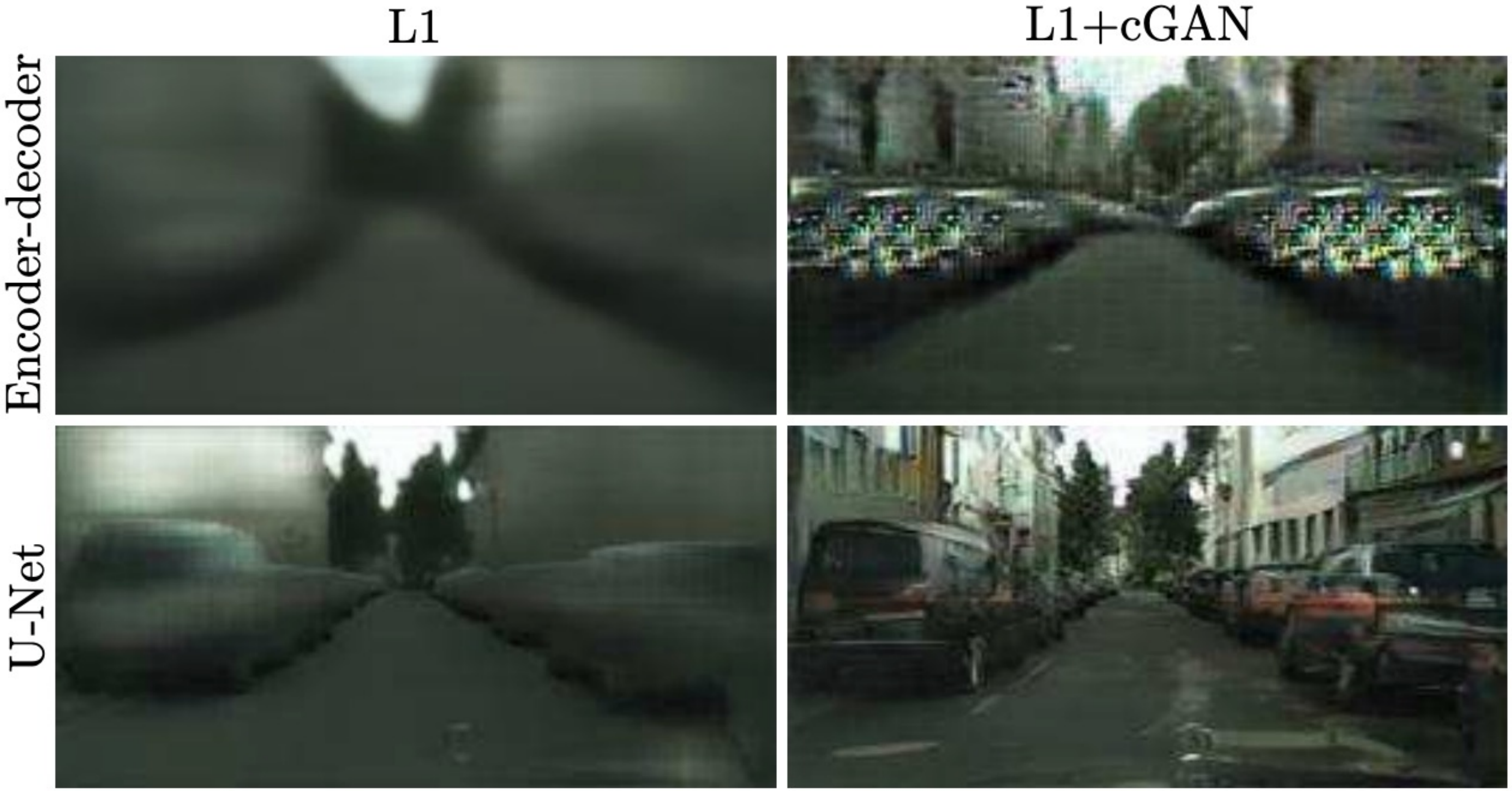


Isola et al. CVPR 2017: Image-to-Image Translation with Conditional Adversarial Networks

Conditional GANs: Also Hard to Train

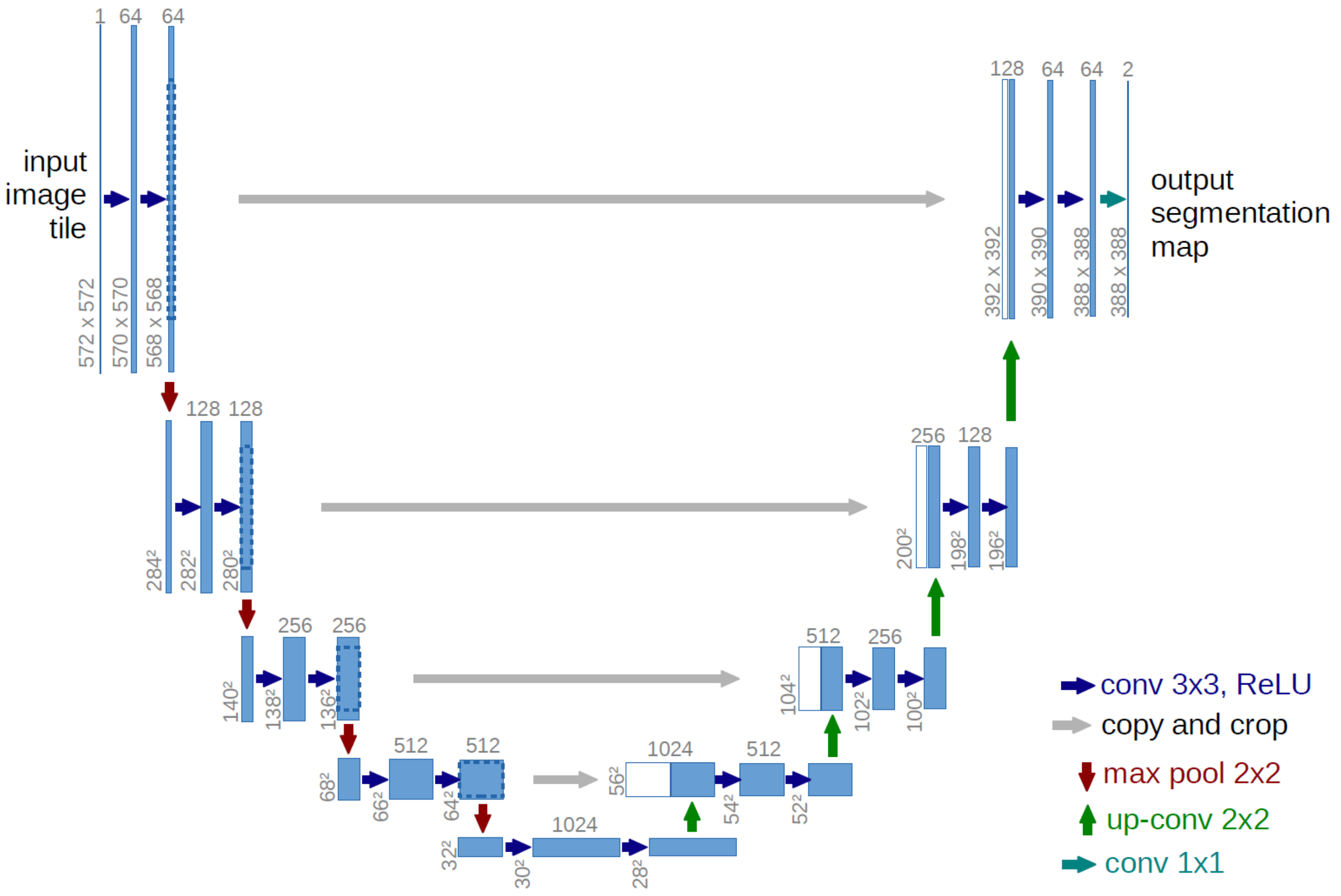
Result they obtained with a regular Fully Convolutional Network

Result they obtained with a U-Net network (with skip-connections)



Isola et al. CVPR 2017: Image-to-Image Translation with Conditional Adversarial Networks

Conditional GANs: Also Hard to Train



Ronneberger et al. MICCAI 2015. U-Net: Convolutional Networks for Biomedical Image Segmentation

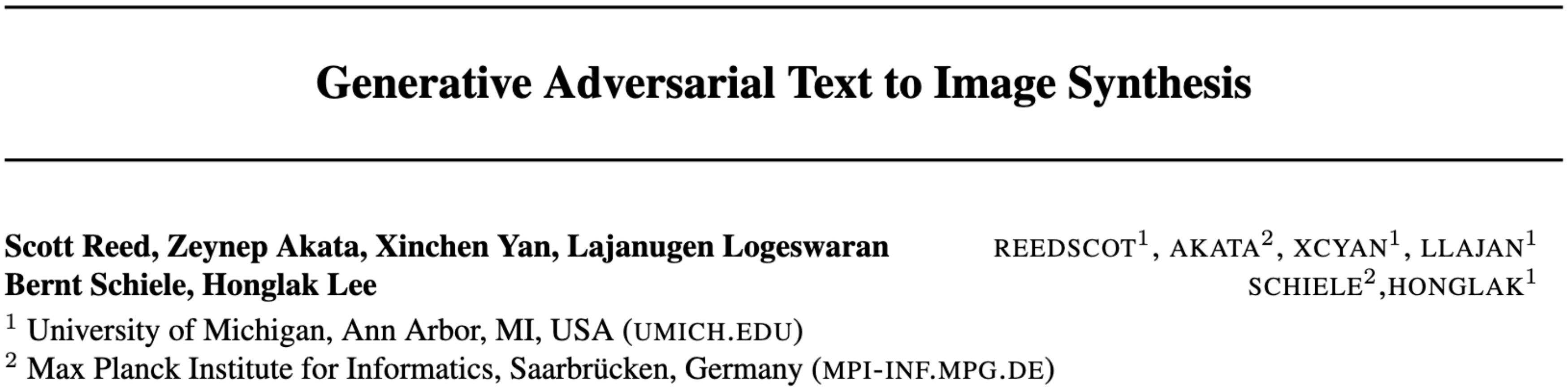
Conditional GANs / Text-conditioned

AttnGAN: Fine-Grained Text to Image Generation with Attentional Generative Adversarial Networks

Tao Xu*[1], Pengchuan Zhang[2], Qiuyuan Huang[2],
Han Zhang[3], Zhe Gan[4], Xiaolei Huang[1], Xiaodong He[2]

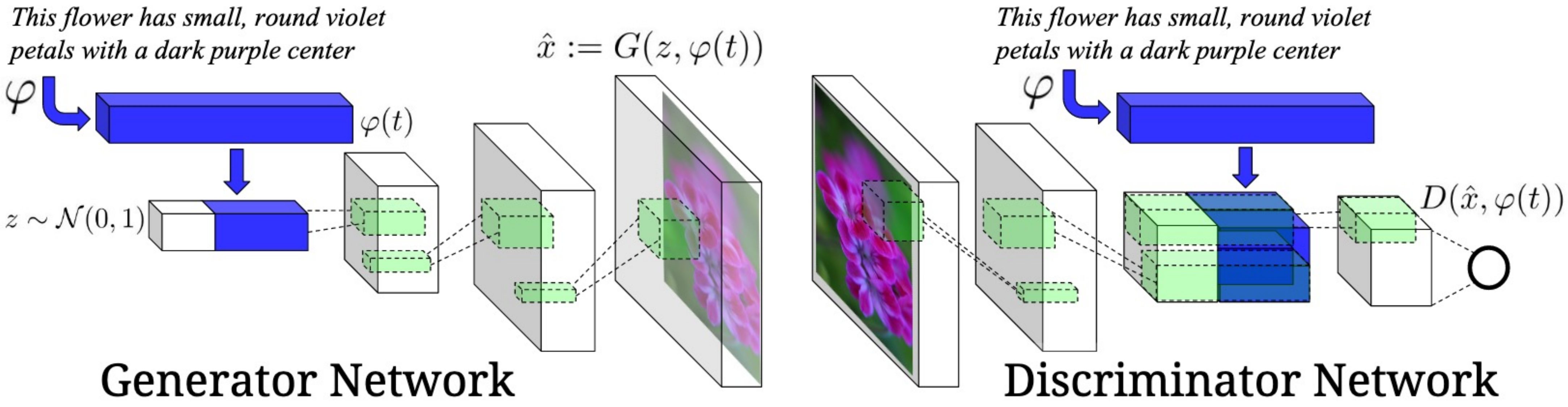
[1]Lehigh University [2]Microsoft Research [3]Rutgers University [4]Duke University
{tax313, xih206}@lehigh.edu, {penzhan, qihua, xiaohe}@microsoft.com
han.zhang@cs.rutgers.edu, zhe.gan@duke.edu

Conditional GANs / Text-conditioned


Generative Adversarial Text to Image Synthesis

Scott Reed, Zeynep Akata, Xinchen Yan, Lajanugen Logeswaran REEDSCOT[1], AKATA[2], XCYAN[1], LLAJAN[1]
Bernt Schiele, Honglak Lee SCHIELE[2],HONGLAK[1]
[1] University of Michigan, Ann Arbor, MI, USA (UMICH.EDU)
[2] Max Planck Institute for Informatics, Saarbrücken, Germany (MPI-INF.MPG.DE)

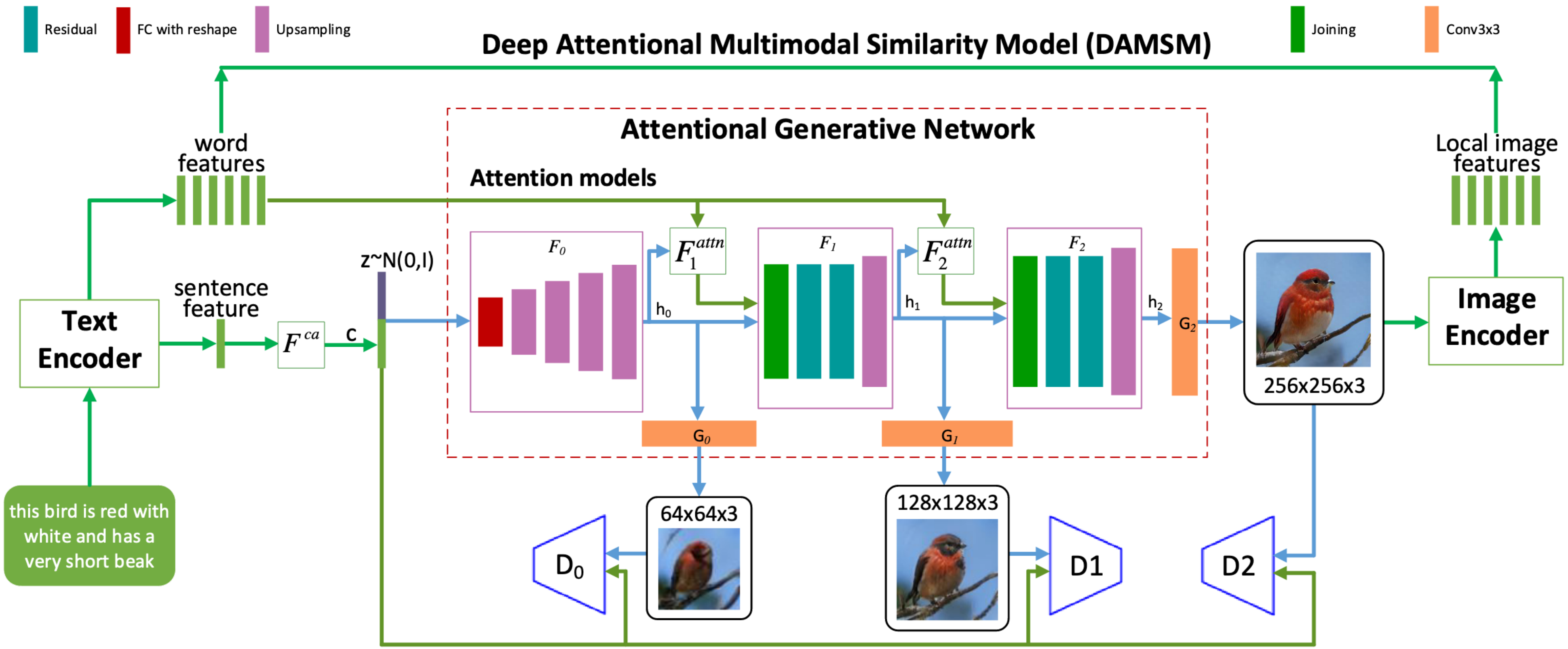
Conditional GANs / Text-conditioned



Conditional GANs / Text-conditioned

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

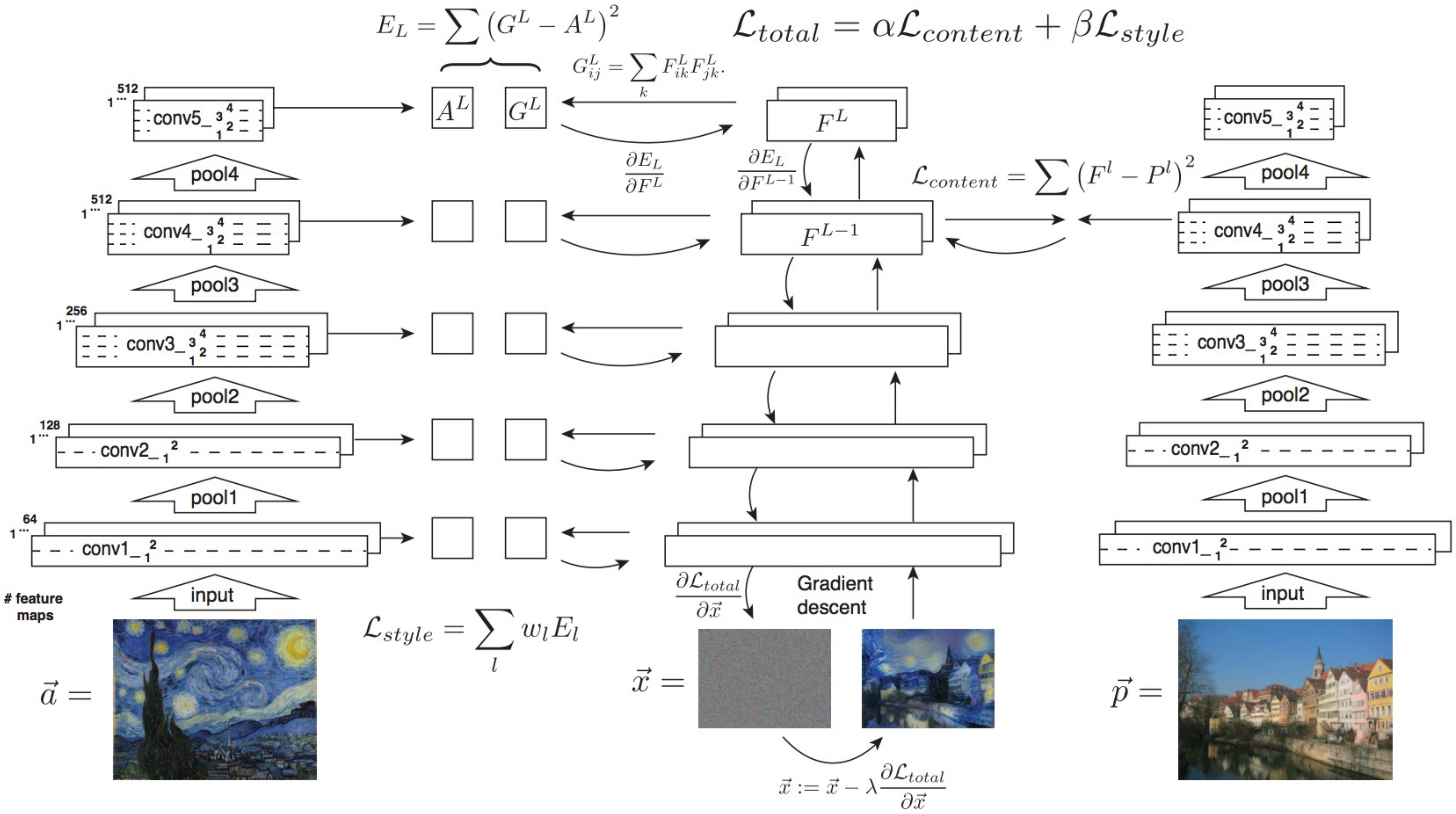
Conditional GANs / Text-conditioned



Conditional GANs / Text-conditioned

More on the Idea of Feature Space Optimization

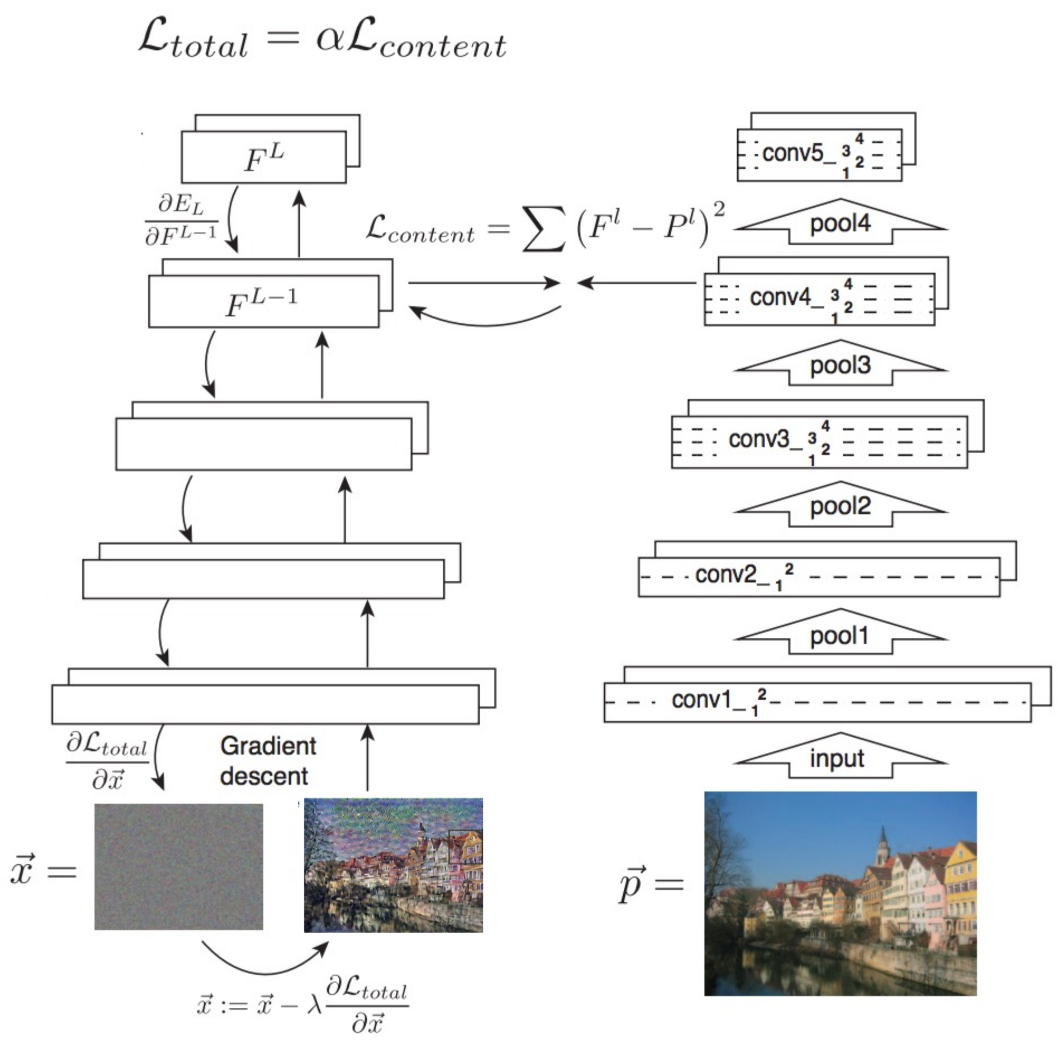
Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016



$E_L = \sum (G^L - A^L)^2$
$\mathcal{L}_{total} = \alpha \mathcal{L}_{content} + \beta \mathcal{L}_{style}$
$G^L_{ij} = \sum_k F^L_{ik} F^L_{jk}.$
A^L
G^L
F^L
F^{L-1}
$\frac{\partial E_L}{\partial F^L}$
$\frac{\partial E_L}{\partial F^{L-1}}$
$\mathcal{L}_{content} = \sum (F^l - P^l)^2$
conv5_1 2 3 4
pool4
conv4_1 2 3 4
pool3
conv3_1 2 3 4
pool2
conv2_1 2
pool1
conv1_1 2
input
512
512
256
128
64
feature maps
$\mathcal{L}_{style} = \sum_l w_l E_l$
$\frac{\partial \mathcal{L}_{total}}{\partial \vec{x}}$
Gradient descent
$\vec{a} =$
$\vec{x} =$
$\vec{p} =$
$\vec{x} := \vec{x} - \lambda \frac{\partial \mathcal{L}_{total}}{\partial \vec{x}}$

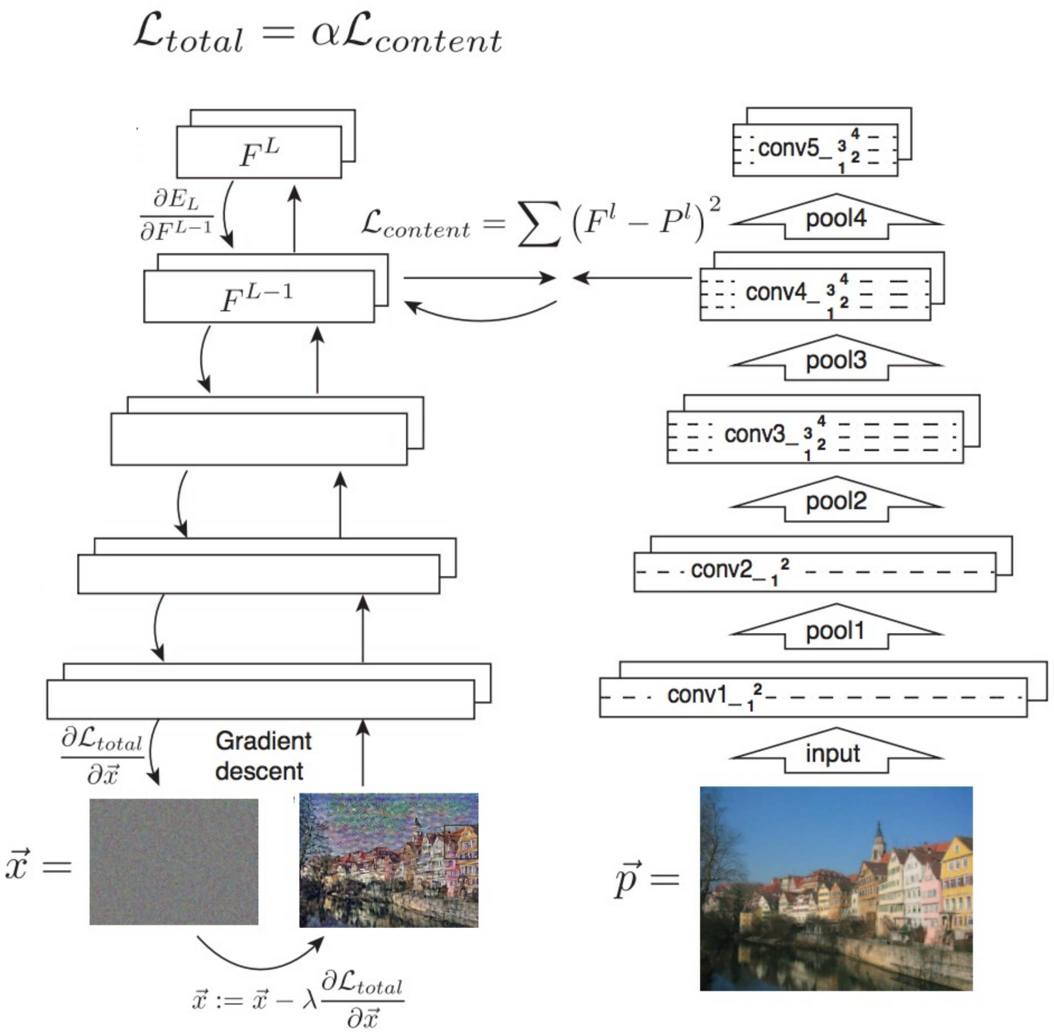
Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016

Idea 1: Image Reconstruction from Features



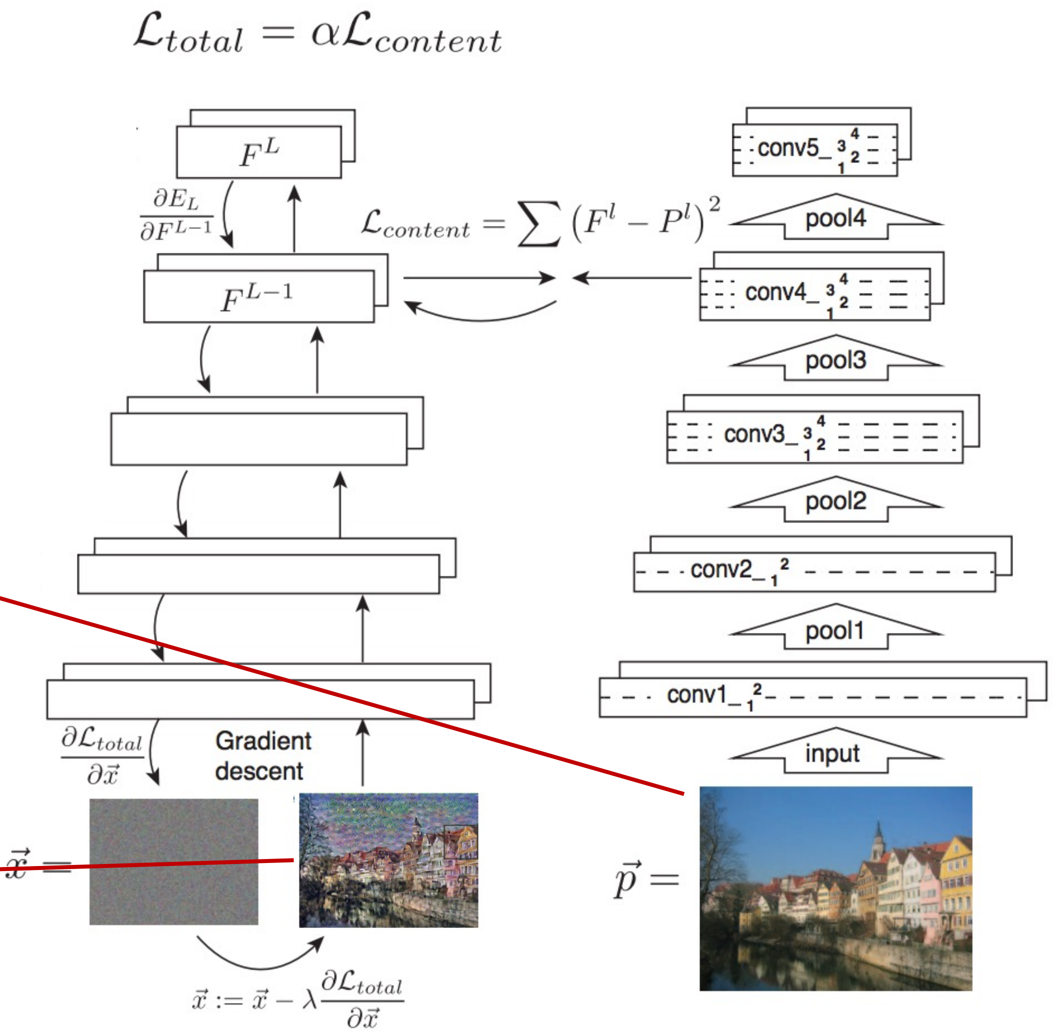
Idea 1: Image Reconstruction from Features

$$\mathcal{L}_{content} = \sum (F^l - P^l)^2$$



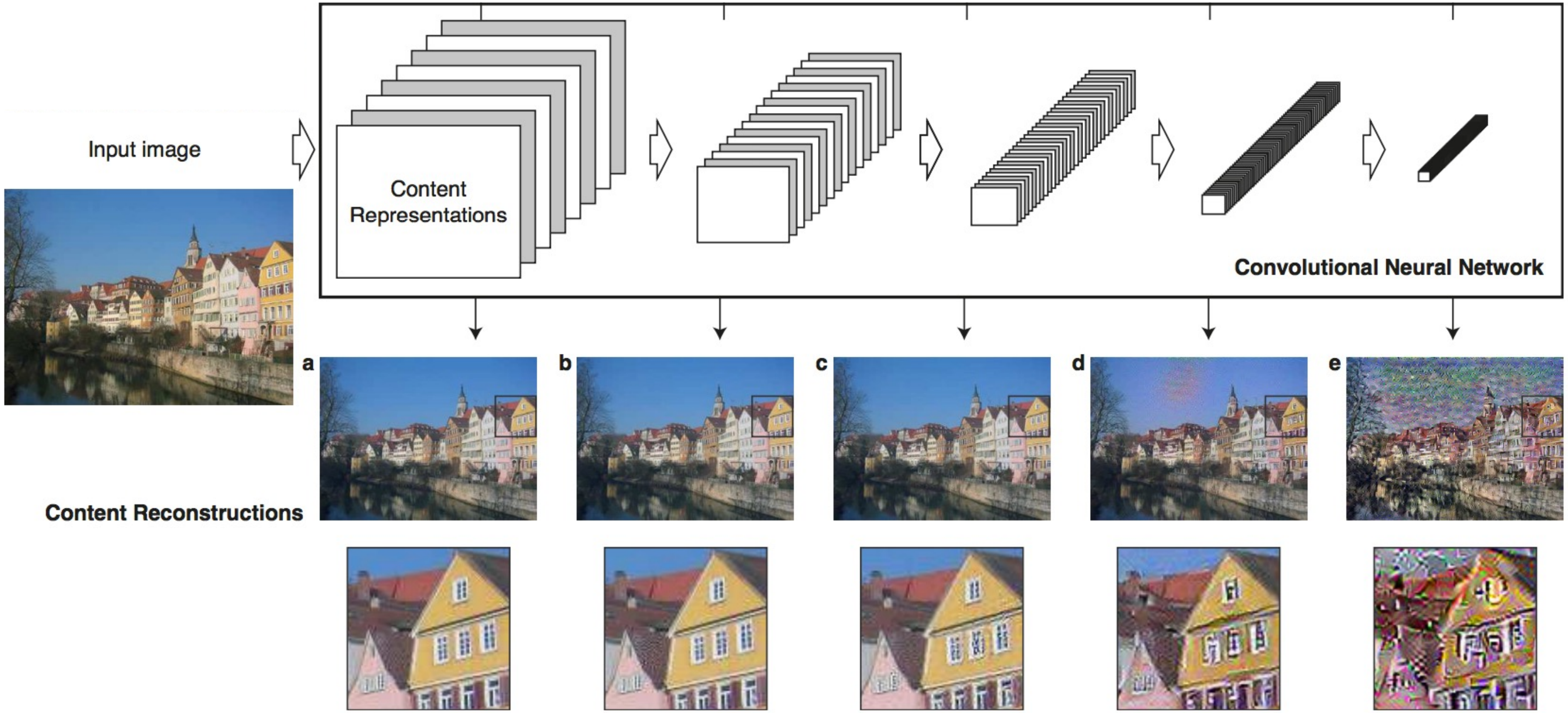
Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016

Idea 1: Image Reconstruction from Features

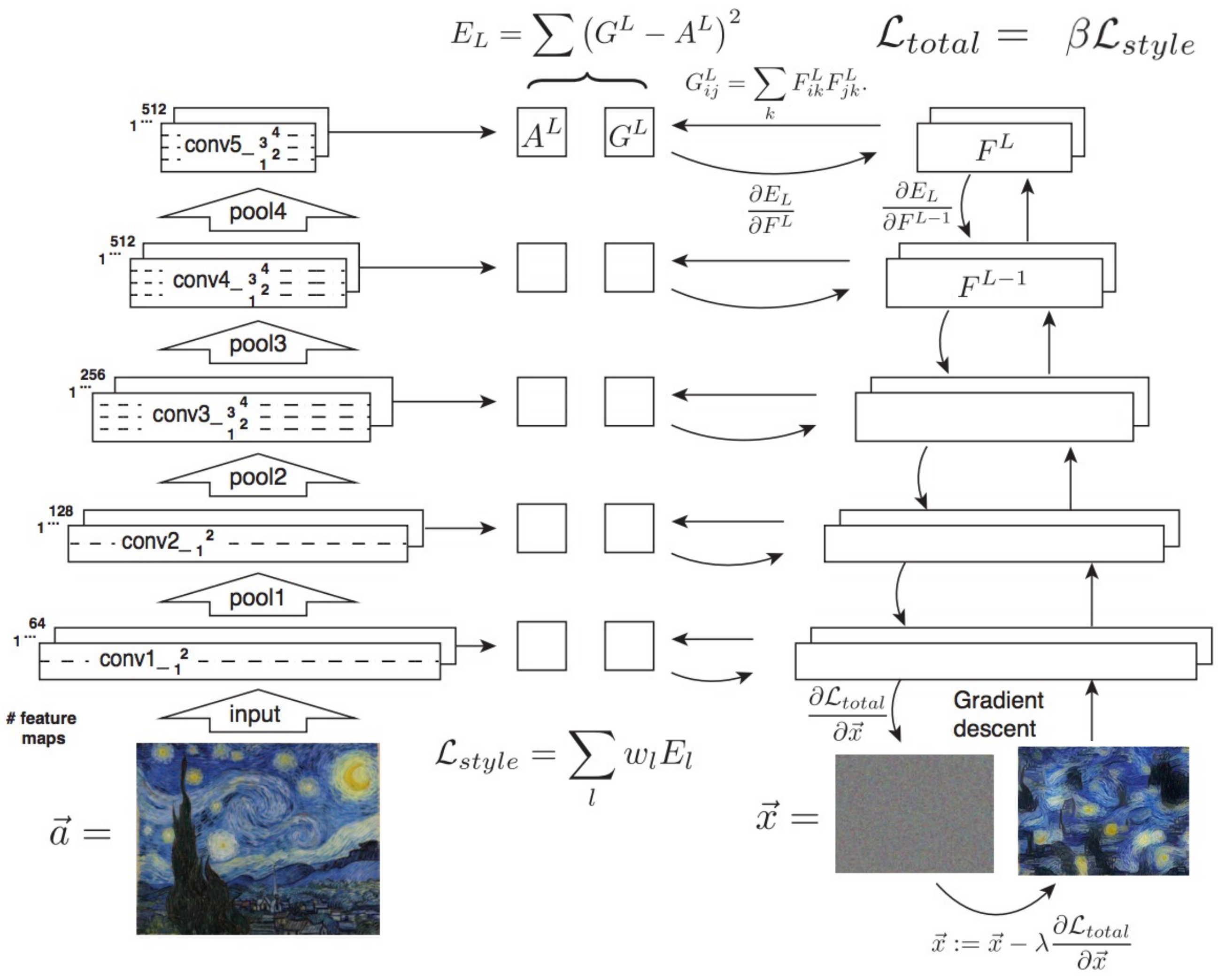


Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016

$$\mathcal{L}_{content} = \sum \left(F^l - P^l\right)^2$$

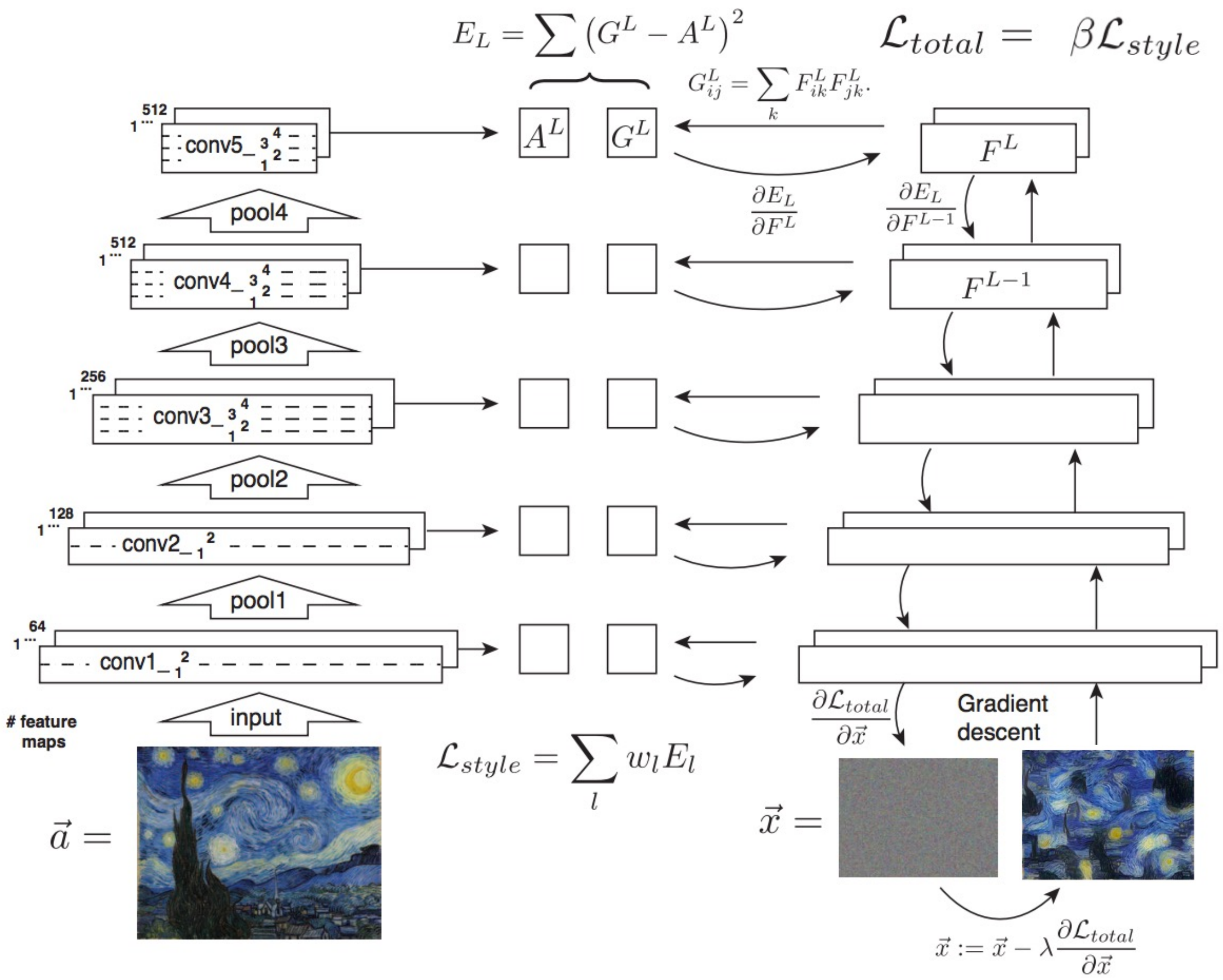


Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016



Idea 2: Backpropagation of Style

Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016



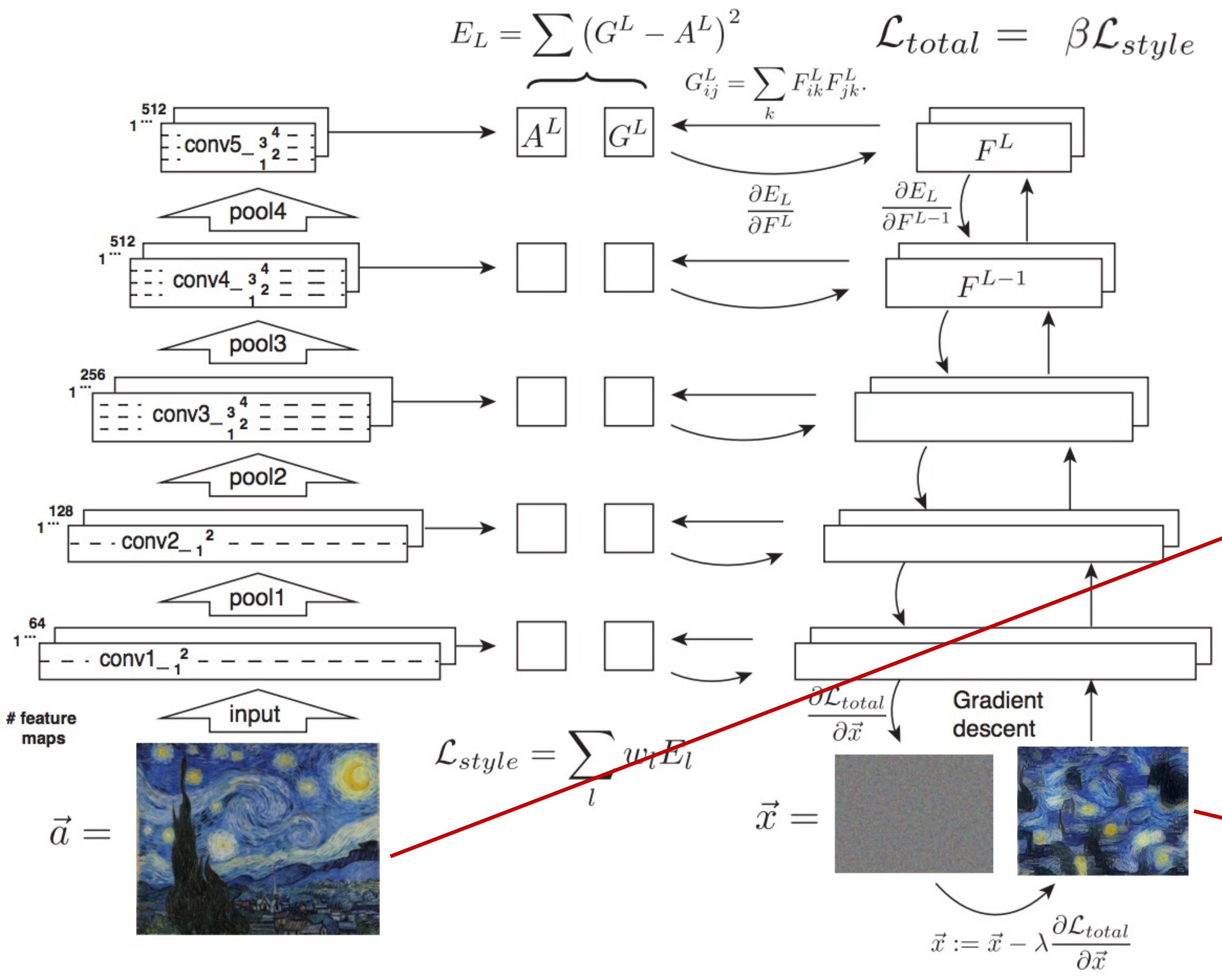
Idea 2: Backpropagation of Style

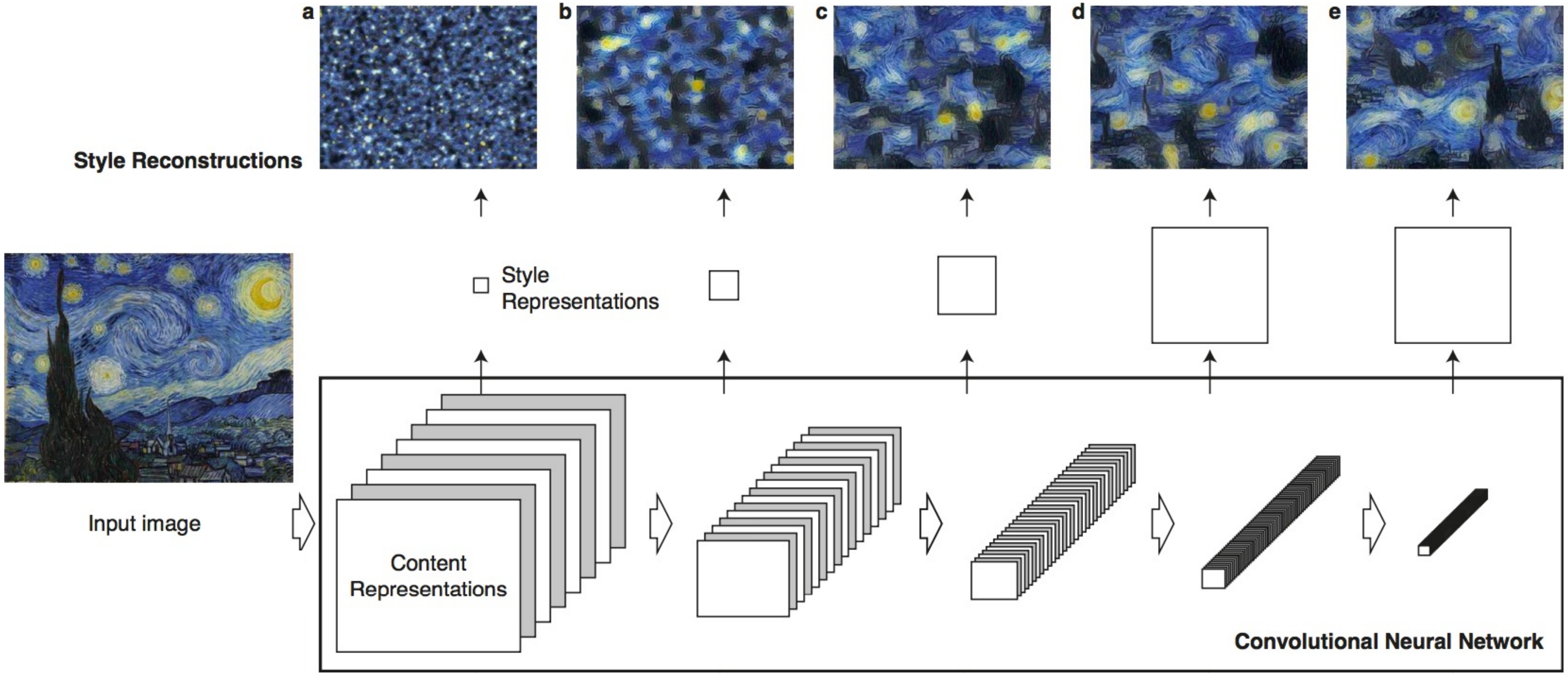
$$G^l_{ij} = \sum_k F^l_{ik} F^l_{jk}.$$

$$E_L = \sum (G^L - A^L)^2$$

Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016

Idea 2: Backpropagation of Style



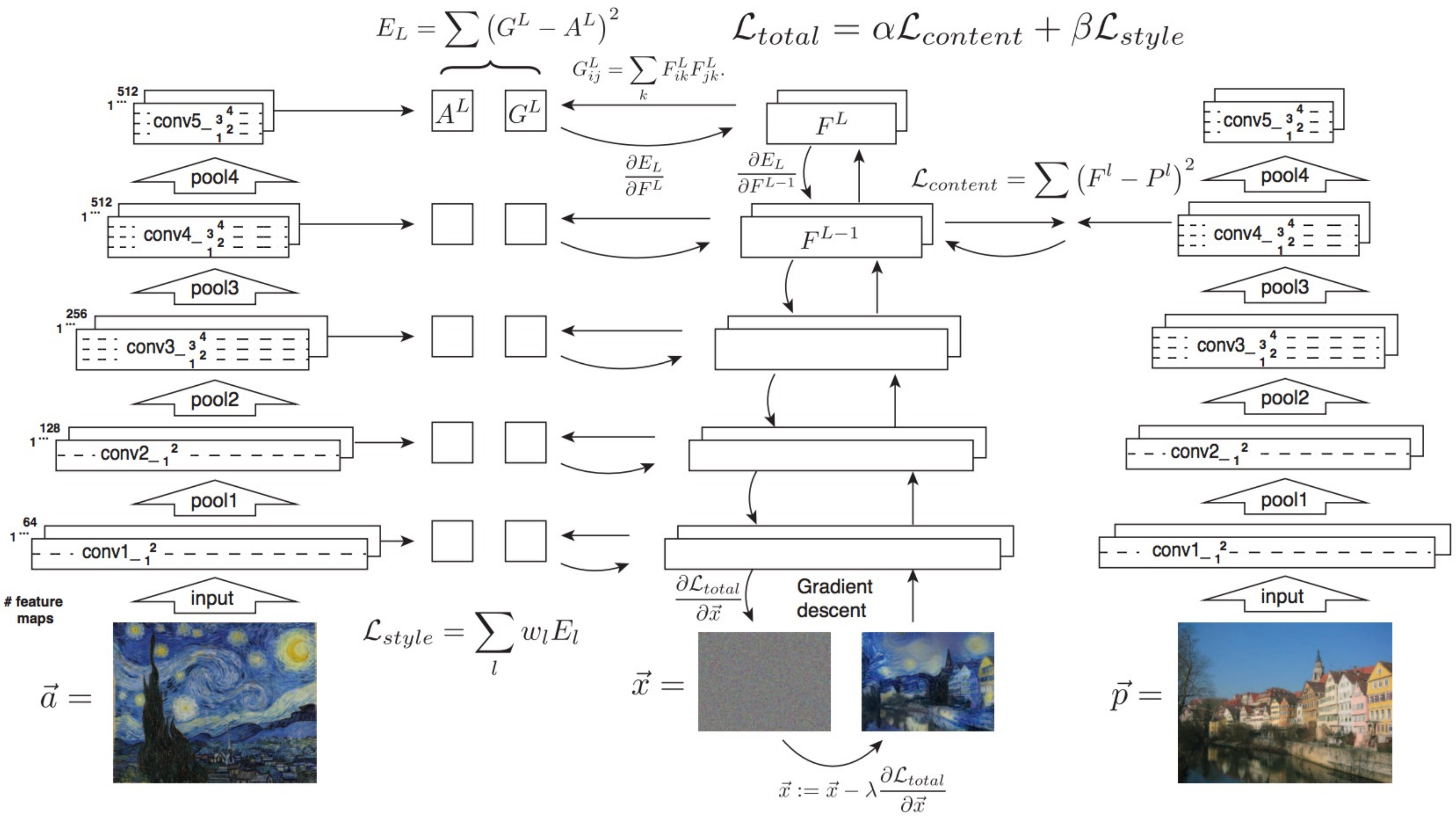


$$G_{ij}^{l} = \sum_{k} F_{ik}^{l} F_{jk}^{l}.$$

$$E_L = \sum \left(G^L - A^L\right)^2$$

Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016

Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016



Gatys et. al. Image Style Transfer Using Convolutional Neural Networks. CVPR 2016

Questions