

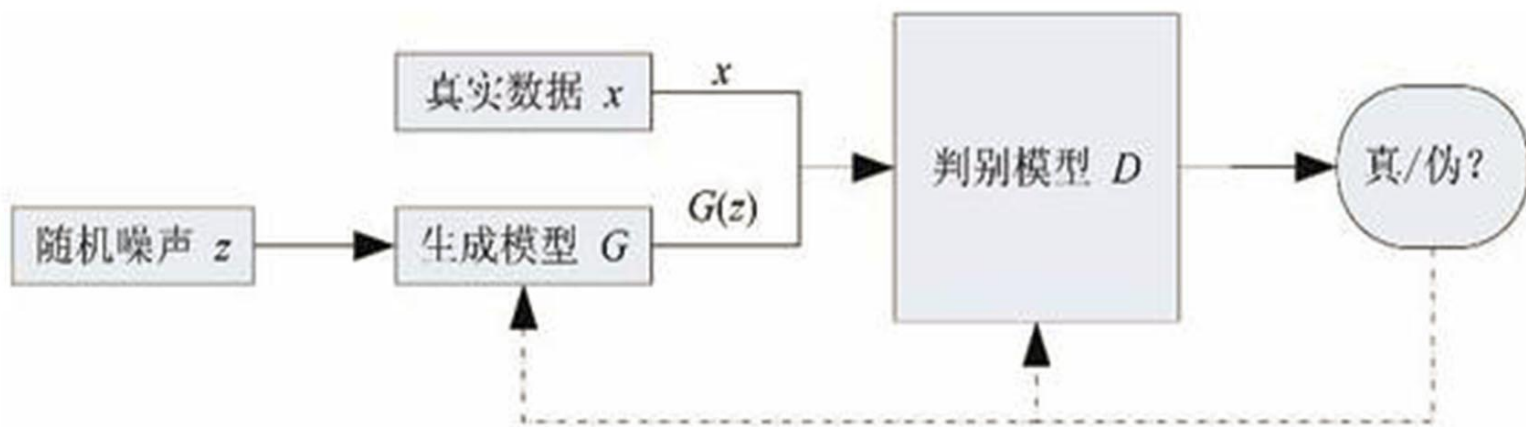
生成对抗网络(GAN)

主要内容

- GAN基本原理
- DCGAN基本原理

GAN的基本原理

- 整个GAN网络由一个**生成器G**（generator）和一个**判别器D**（discriminator）构成
 - 生成器捕捉真实数据样本的潜在分布，并生成新的数据样本
 - 判别器是一个二分类器，判别输入是真实数据还是生成的样本



GAN的基本原理

■ 输入：

- 生成器G：随机噪声分布 z (通常为高斯噪声分布)
- 判别器D：真实数据 x 以及生成器生成造假数据 $G(z)$

■ 输出：

- 当判别器D判别概率等于0.5时，输出 $G(z)=x$

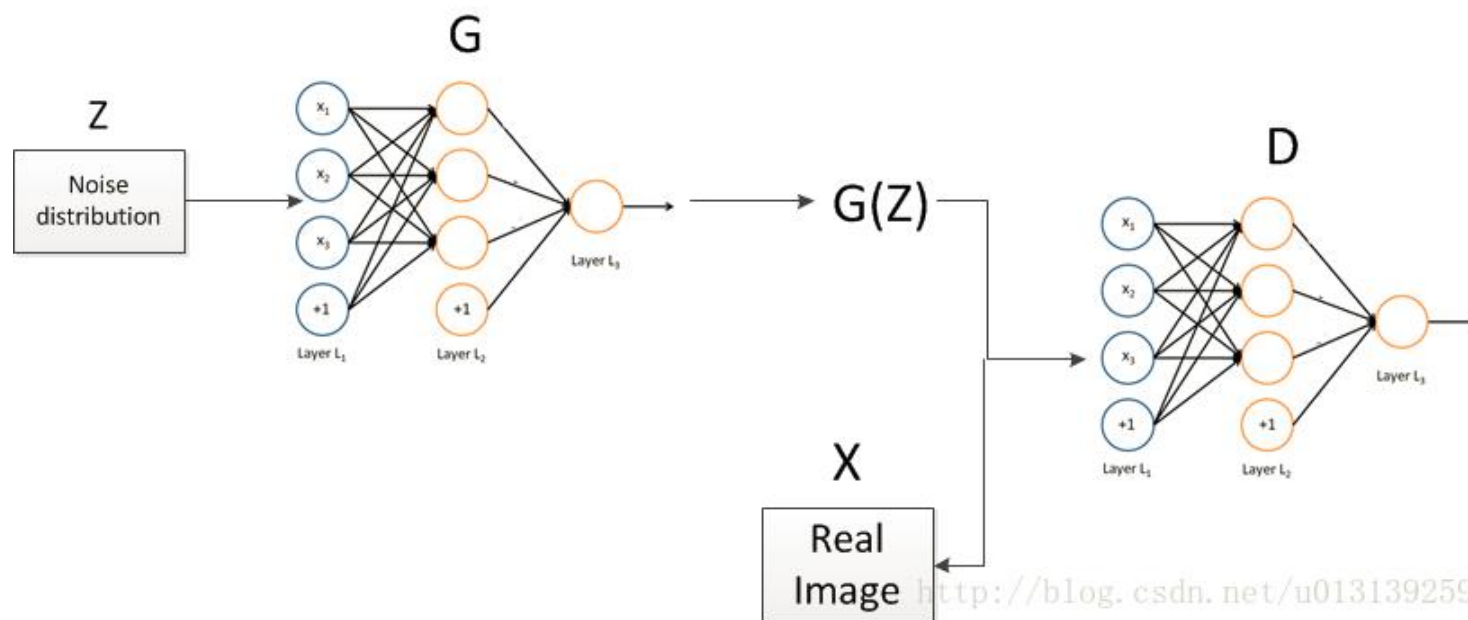
■ 目标函数 $\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$

- max放在里面一是表明先对判别器D 进行训练，二是实验表明这样效果比较好，若min在内部容易产生过拟合问题。

- 判别器D的目的是正确区分出 $P_{\text{data}}(x)$ 和 $P_z(z)$ ，因此判别器D努力的**增加** $D(x)$ ，并且**减小** $D(G(z))$ （即增大 $(1-D(G(z)))$ ）因为， $D() \in [0, 1]$ ，因此要 $\max V(G, D)$

- 生成器G是要**增大** $D(G(z))$ （即减小 $(1-D(G(z)))$ ），若 $C(G) = \max V(D, G)$ ，所以要 $\min C(G)$

GAN的基本原理



GAN的基本原理

Image Generation

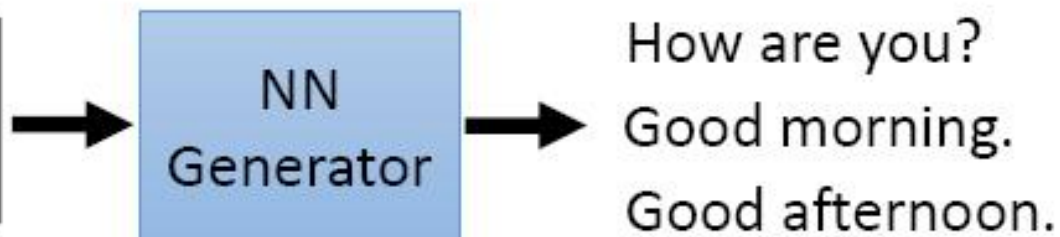
$$\begin{bmatrix} 0.3 \\ -0.1 \\ \vdots \\ -0.7 \end{bmatrix} \begin{bmatrix} 0.1 \\ -0.1 \\ \vdots \\ 0.7 \end{bmatrix} \begin{bmatrix} -0.3 \\ 0.1 \\ \vdots \\ 0.9 \end{bmatrix}$$

In a specific range

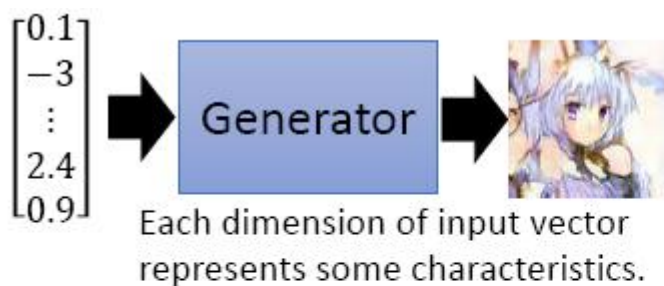
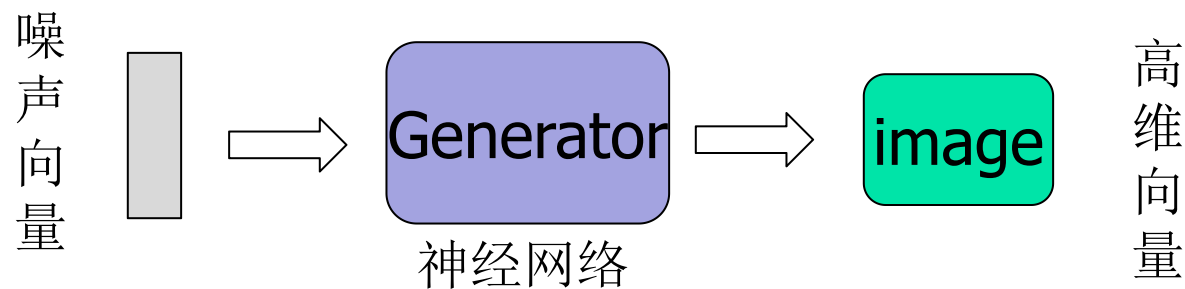


Sentence Generation

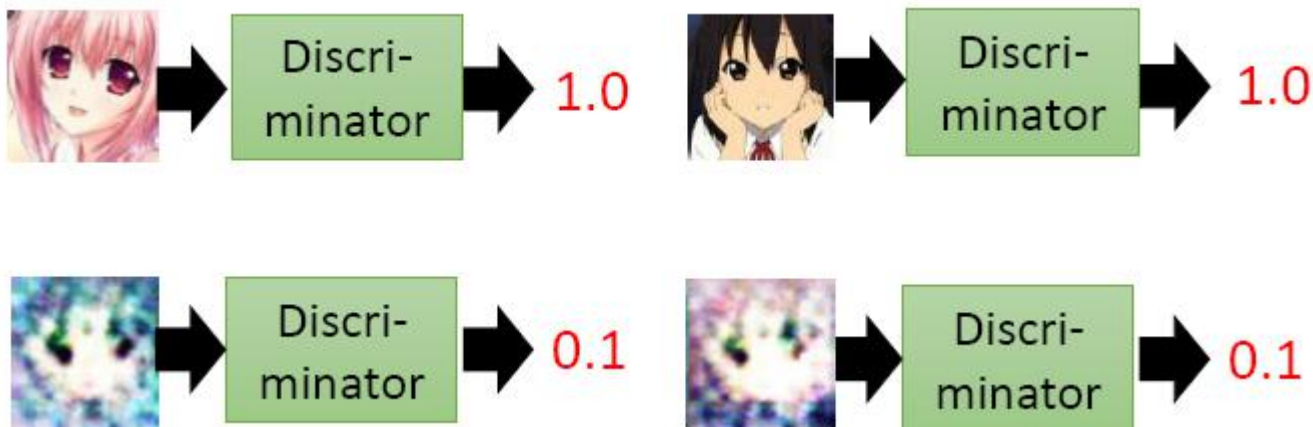
$$\begin{bmatrix} 0.3 \\ -0.1 \\ \vdots \\ -0.7 \end{bmatrix} \begin{bmatrix} 0.1 \\ -0.1 \\ \vdots \\ 0.2 \end{bmatrix} \begin{bmatrix} -0.3 \\ 0.1 \\ \vdots \\ 0.5 \end{bmatrix}$$



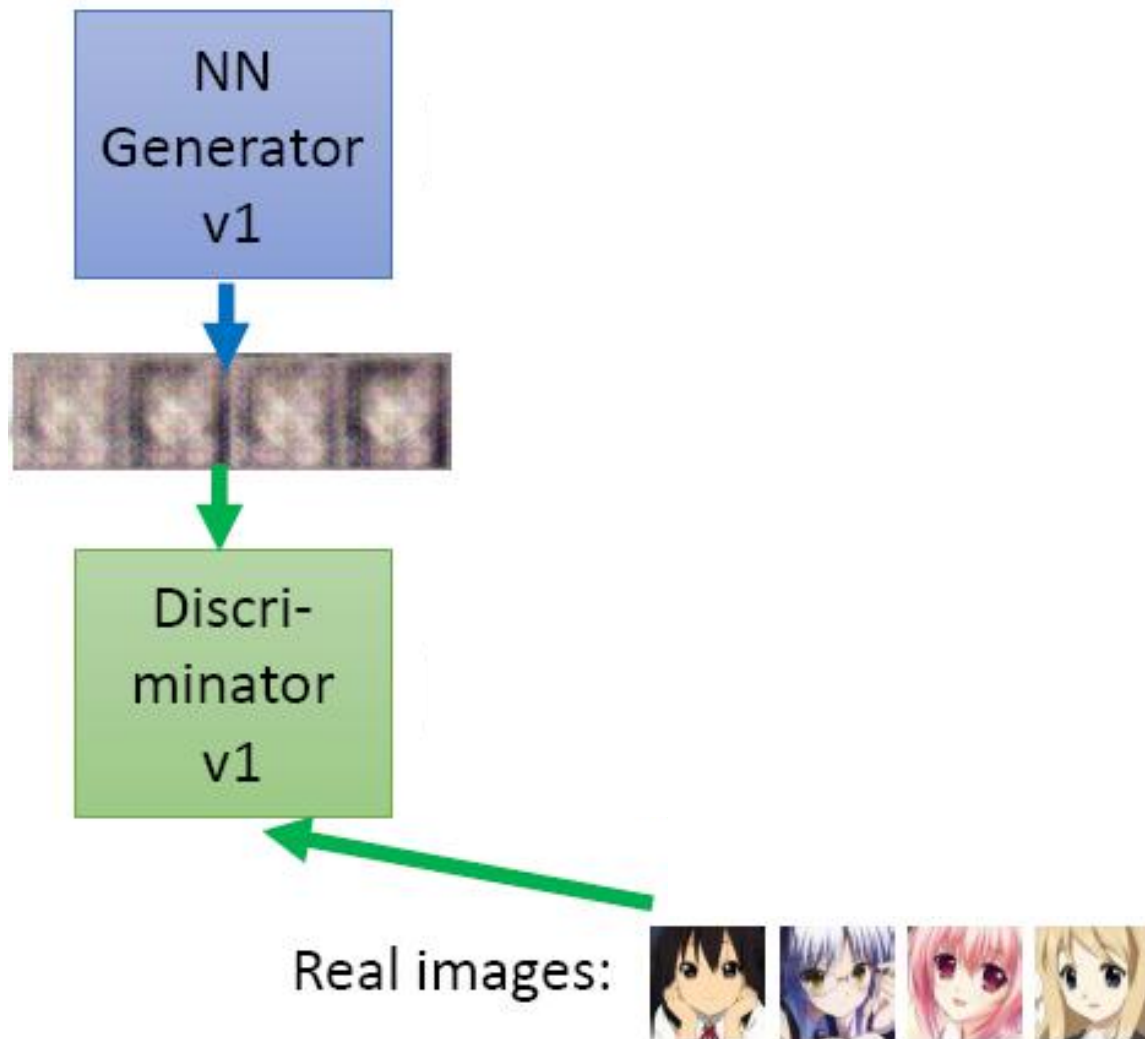
GAN的基本原理



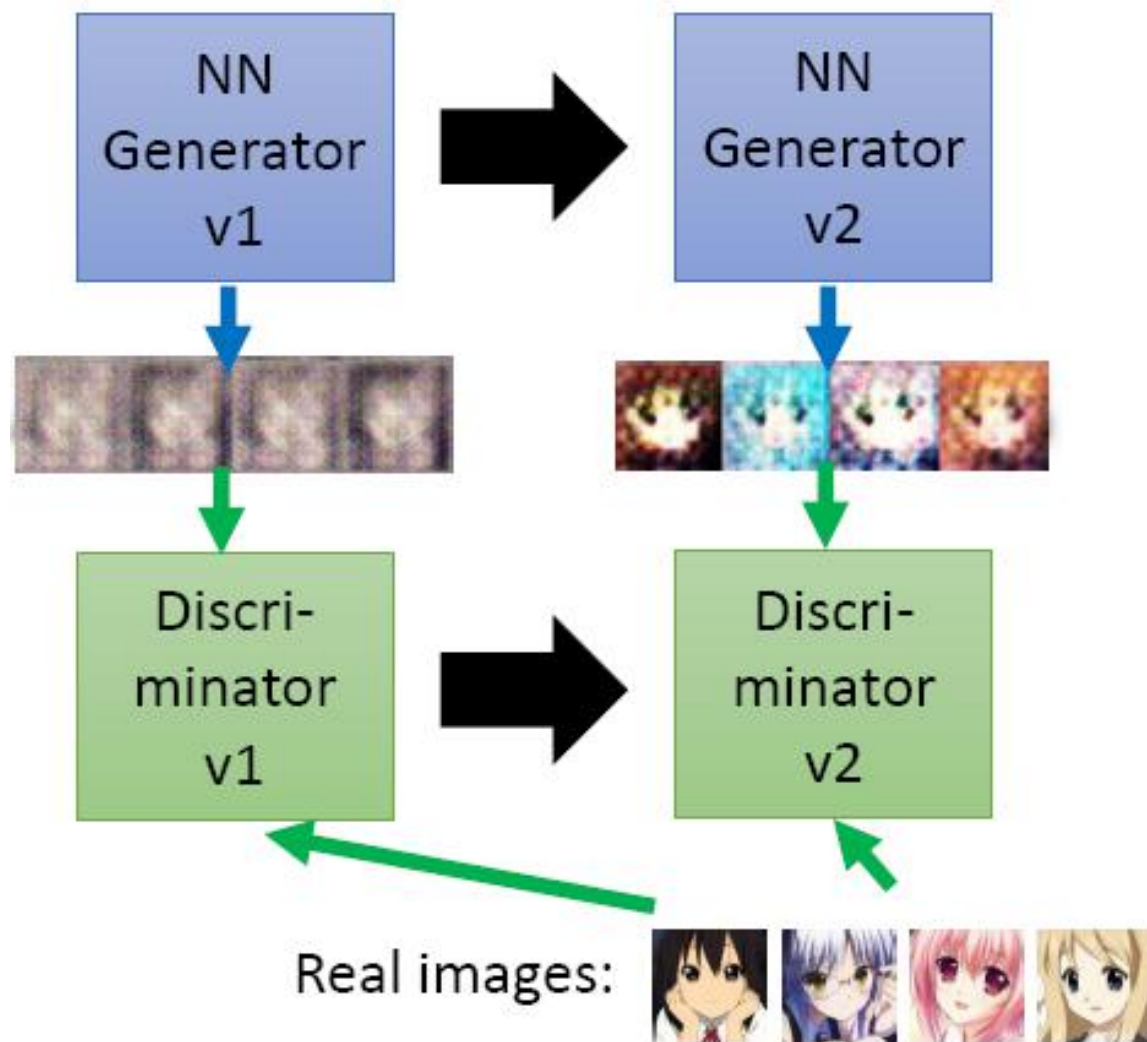
GAN的基本原理



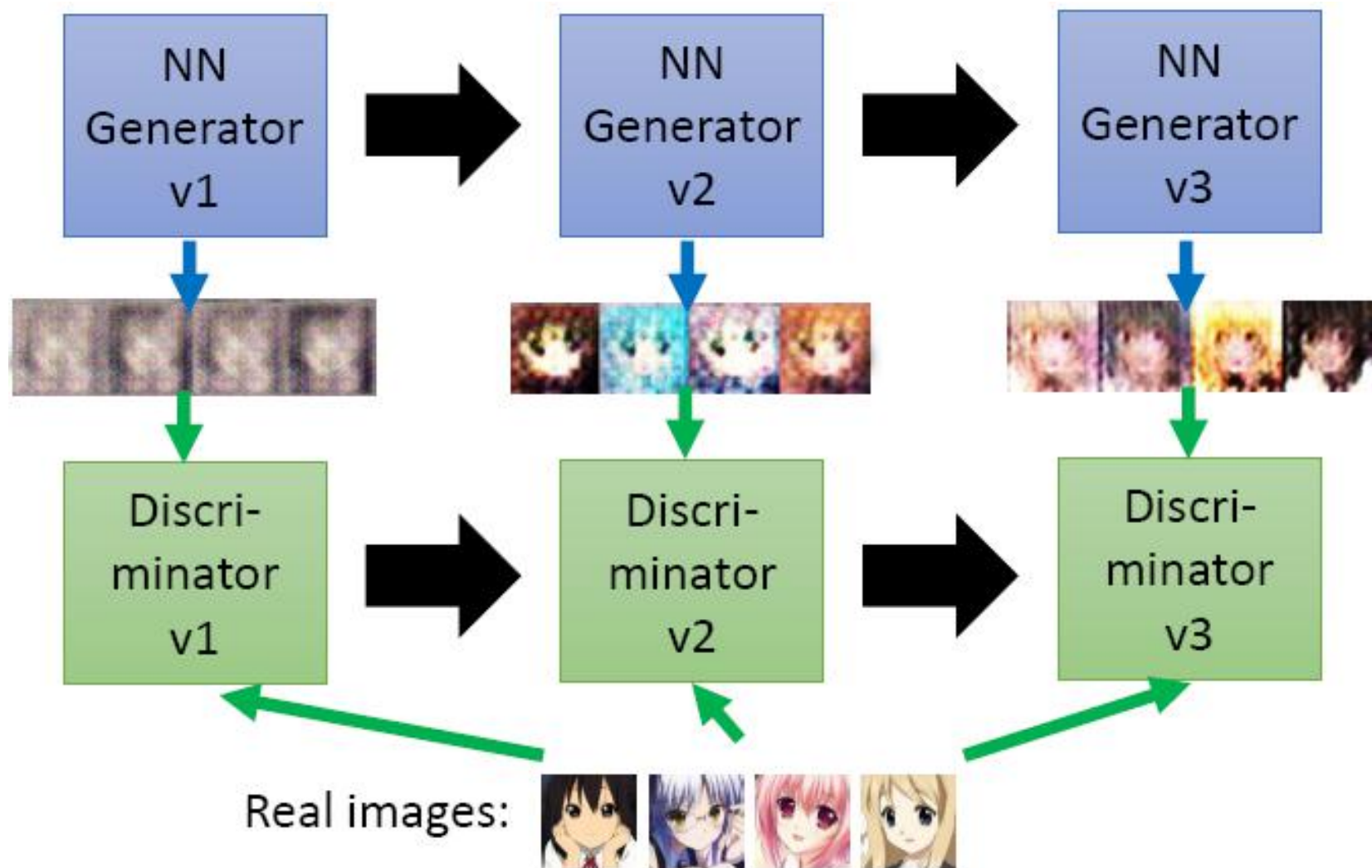
GAN的基本原理



GAN的基本原理



GAN的基本原理

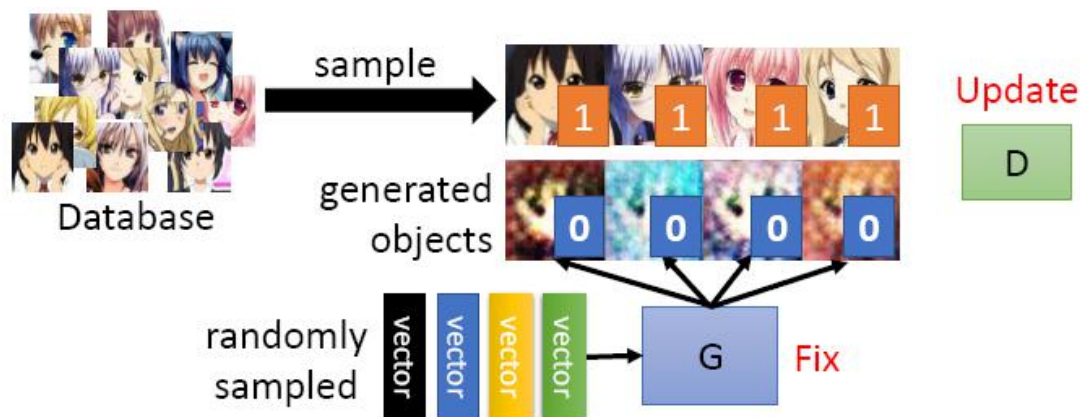


GAN的基本原理

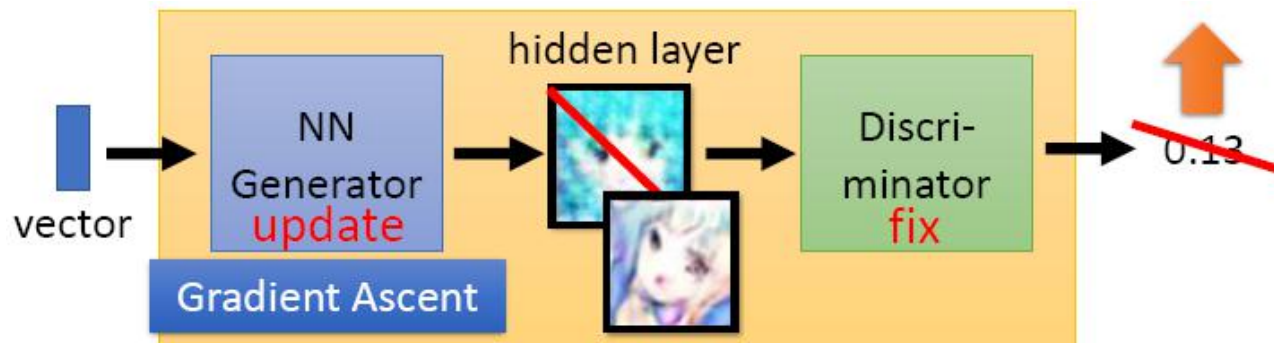
- 初始化G和D网络

- 对于每一次迭代训练:

(1) 固定G, 更新D: 对于真实数据判别输出接近1, 对于生成数据判别输出接近0



(2) 固定D, 更新G: 通过更新G, 使得D判别输出值逐渐接近1



GAN的基本原理

Algorithm Initialize θ_d for D and θ_g for G

- In each training iteration:

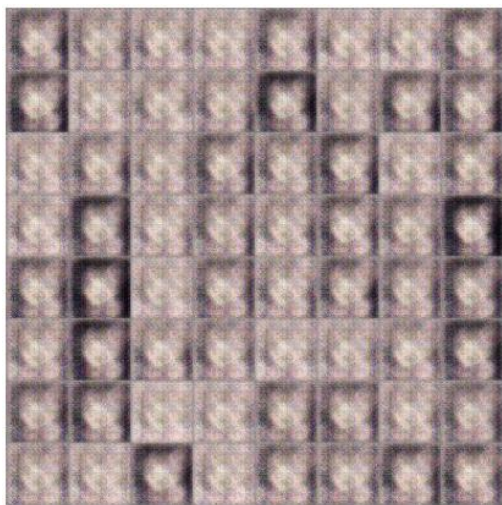
Learning
D

- Sample m examples $\{x^1, x^2, \dots, x^m\}$ from database
- Sample m noise samples $\{z^1, z^2, \dots, z^m\}$ from a distribution
- Obtaining generated data $\{\tilde{x}^1, \tilde{x}^2, \dots, \tilde{x}^m\}$, $\tilde{x}^i = G(z^i)$
- Update discriminator parameters θ_d to maximize
 - $\tilde{V} = \frac{1}{m} \sum_{i=1}^m \log D(x^i) + \frac{1}{m} \sum_{i=1}^m \log (1 - D(\tilde{x}^i))$
 - $\theta_d \leftarrow \theta_d + \eta \nabla \tilde{V}(\theta_d)$

Learning
G

- Sample m noise samples $\{z^1, z^2, \dots, z^m\}$ from a distribution
- Update generator parameters θ_g to maximize
 - $\tilde{V} = \frac{1}{m} \sum_{i=1}^m \log (D(G(z^i)))$
 - $\theta_g \leftarrow \theta_g - \eta \nabla \tilde{V}(\theta_g)$

GAN的基本原理



100



1000



2000



5000



20000



50000

GAN的基本原理



最终生成图像
以假乱真

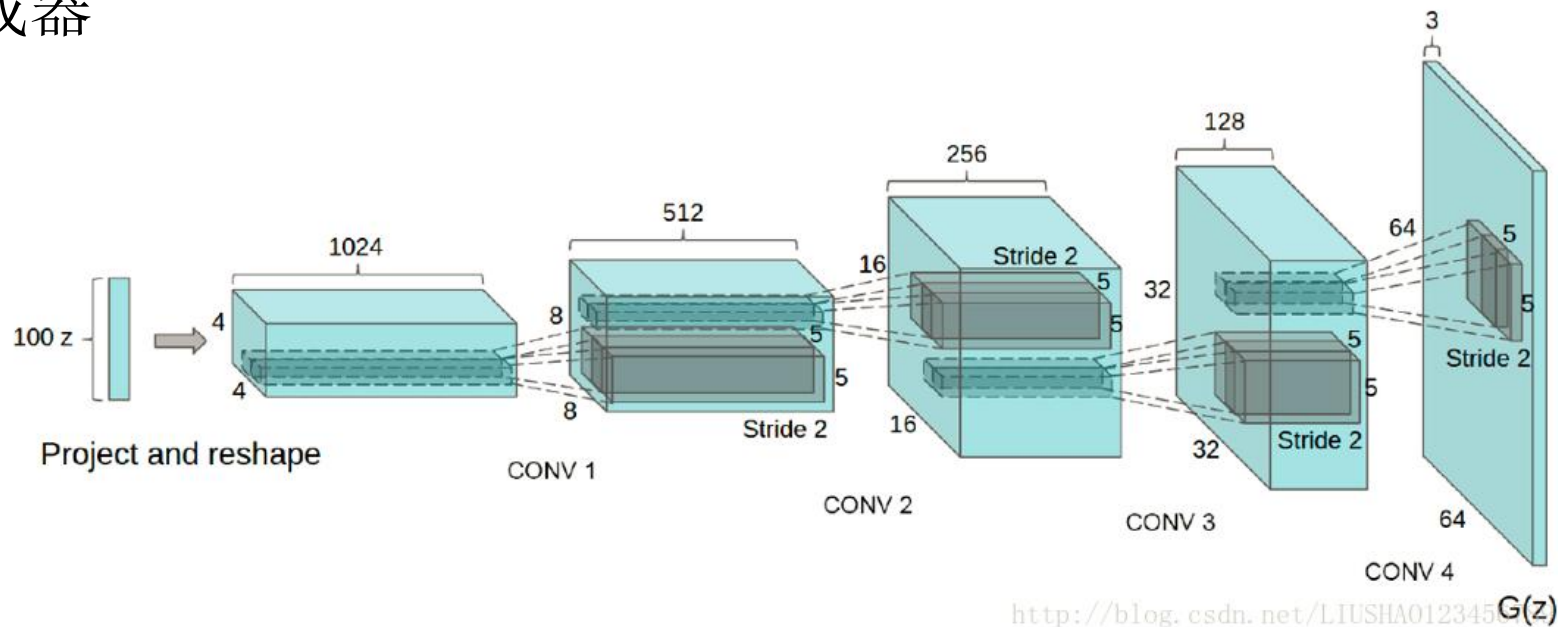
DCGAN

基本特点

- pooling层由卷积层代替
- 在G和D网络上都使用Batch Normalization
 - BN本质就是通过规范化方法，把每层神经网络任意神经元这个输入值的分布强行拉回到均值为0方差为1的标准正态分布
 - 解决初始化差的问题
 - 帮助梯度传播到每一层
 - 防止G网络把所有的样本都收敛到同一个点
- 在CNN中移除全连接层
- 在G网络输出层使用tanh,其他所有层使用Relu
- 在D网络的所有层使用leakyRelu

DCGAN基本原理

生成器

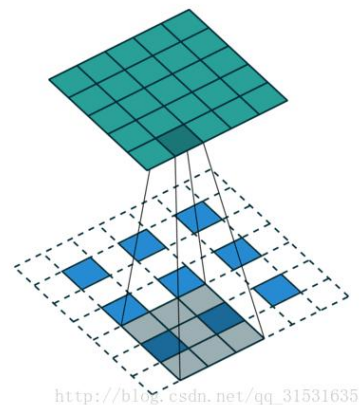
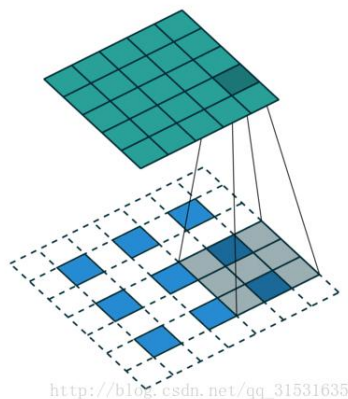
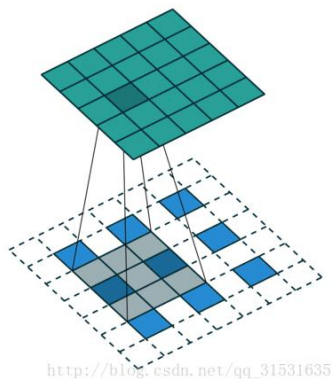
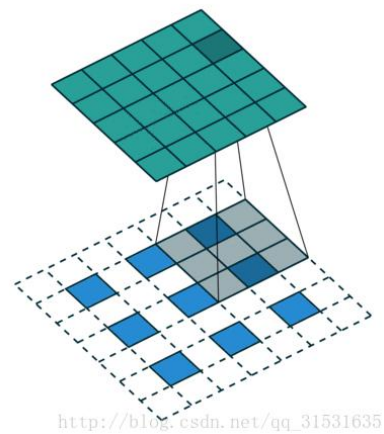
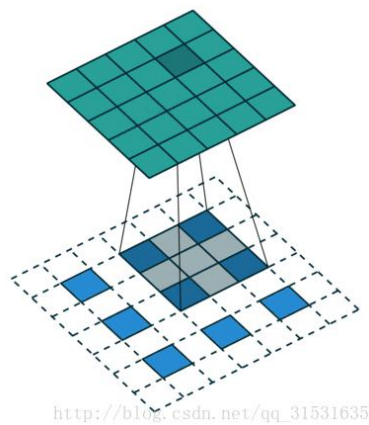
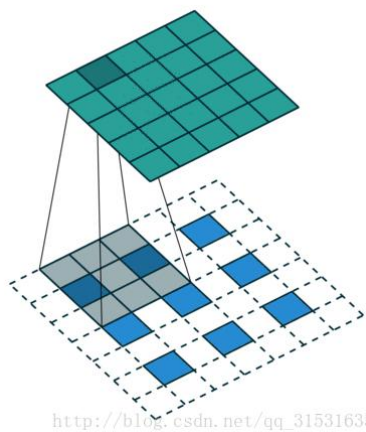


- 利用CNN作为一个生成器G，输入是噪声分布，通过反卷积升维最终得到一个图片大小和真实样本数据（图片）大小相同都为64x64x3，即长宽都为64的RGB三通道彩色图片。
- 反卷积过程：即在原有像素上进行上采样，就是在其周围填充0，白色方块代表0像素，蓝色方块代表原始像素

DCGAN基本原理

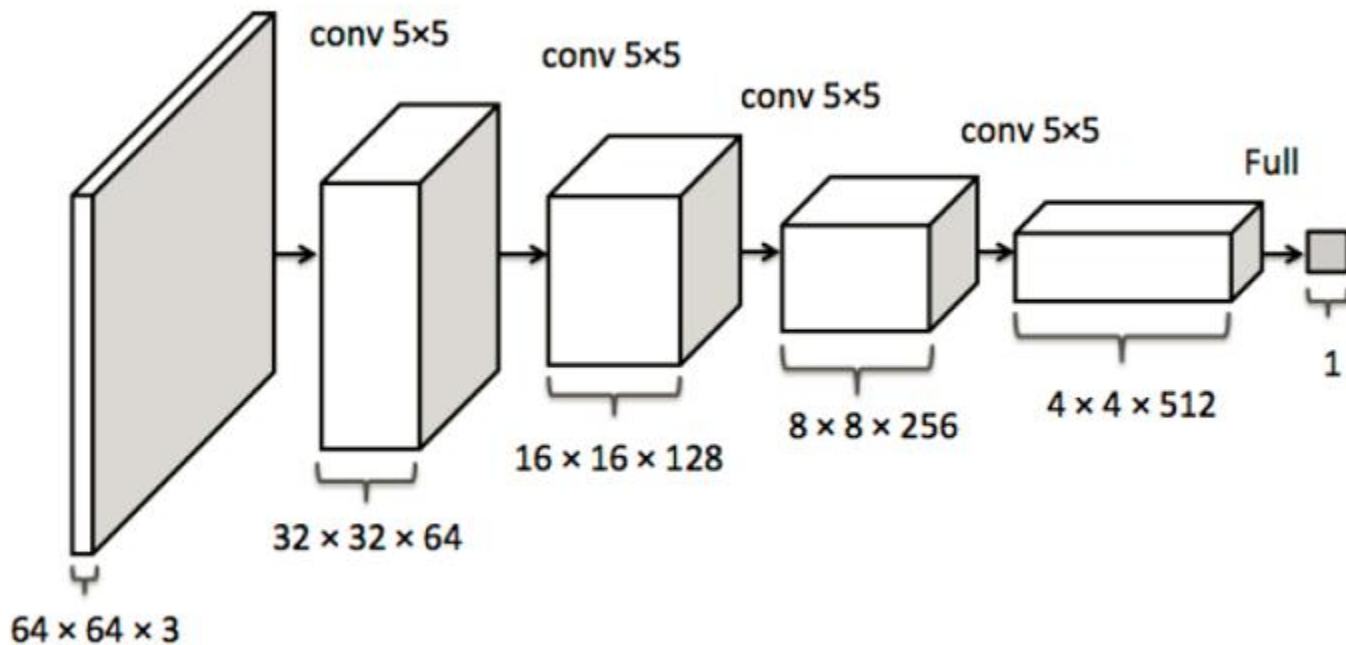
■ 反卷积

- 把卷积的前向传播和反向传播完全颠倒
- 即在原有像素上进行上采样，就是在其周围填充0，白色方块代表0像素，蓝色方块代表原始像素



DCGAN基本原理

判别器



- 使用带步长的卷积（strided convolutions）取代了的池化（spatial pooling），容许网络学习自己的空间下采样（spatial downsampling）
- 判别器D，输入为 $64 \times 64 \times 3$ 的RGB三通道彩色真实样本图片或者造假图片，最后给出结果，1表示真实图片，0表示造假图片

实验平台说明

- 上机实践平台：
 - <http://10.134.171.240>
 - 用户名：学号
 - 初始密码：123456
 - 在“我的课程”进入本课程，第七次实验“生成对抗网络GAN实验”
 - 按要求扩展实验，并提交实验报告
 - 实验报告统一发助教邮箱，实验报告命名“第n次实验-学号-姓名”