# 绪论

## 1.1研究背景及意义

近年来深度学习在许多传统机器学习难以解决的问题上有着优异的表现，尤其在计算机视觉领域，如：人脸识别，自动驾驶，视频检测等。尽管深度学习在计算机视觉领域表现优异，但Christian Szegedy等人发现现有的深度神经网络（Deep Neural Networks，简称DNN）易受对抗样本的攻击，这些对抗样本只是在原有的图像样本添加轻微的扰动（人类视觉无法察觉），可以导致深度神经网络输出错误的分类结果。如图1所示，模型将原始图片识别为猫，在原始图像中加入轻微的对抗样本扰动后，模型将图像识别为鸵鸟。Nguyen 等人还发现一些人类无法识别的样本，深度神经网络模型依旧能够以高置信度对该样本进行分类。除此之外对抗样本的攻击已对现有的深度学习应用领域产生严重威胁，如对人脸识别系统的攻击，攻击者只需在人脸图像上添加经过训练的扰动，就可让人脸识别系统将该图像识别为指定的用户。Kdnuggets指出对抗样本不仅仅存在于深度学习相关领域，也普遍存在于许多机器学习模型中，因此进一步研究对抗样本不仅有利于提高目前已有深度学习解决方案的安全性，还有利于整个机器学习及深度学习领域的发展。

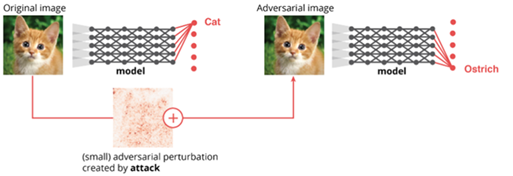


图1 对抗样本攻击举例

目前现实中深度学习解决方案越来越多，对抗样本的存在极大的威胁到这些解决方案。因此在设计深度学习解决方案的过程中，必须考虑到如何防御对抗样本的攻击。现有的防御策略大多通过减轻深度学习模型的过拟合程度来防御对抗样本的攻击，如在训练数据集中添加大量对抗样本。但在减轻深度学习模型的过拟合过程中，大概率会降低模型对纯净图像（无扰动图像）分类准确率。并且需要重新训练整个模型，极大的提高了深度学习模型训练成本。同时对于全新的对抗样本防御效果较差。到目前为止还没有一种高效能防御所有对抗样本攻击的防御方法。并且随着防御策略的升级，攻击的手段也在逐步提高，对抗样本扰动从开始简单针对特定图像的扰动发展到可以添加到任意图像的通用扰动，扰动大小也变的越来越小。

因此目前急需一种在保证深度学习模型对原始图像分类精度和训练成本基本不变的条件下，同时能防御不同种类对抗样本防御策略。针对上述情况，本论文提出基于VAE-GAN的对抗样本防御方法，在保证图像质量基本不变的条件下，对对抗样本进行去噪处理。本方法不仅能有效降低深度学习模型对对抗样的误识别，而且相较于大多数其他防御策略训练成本也较低。

## 1.2研究现状

### 1.2.1生成对抗样本研究现状

2014年Szegedy[2]等人首次提出对样本概念，证明了可以通过对图像添加小量的人类察觉不到的扰动误导神经网络做出误分类。他们尝试求解让深度学习模型做出误分类的最小扰动方程。由于求解该最小扰动程算法复杂度过高，他们将问题转化为寻找最小损失函数添加项方程，成功将问题转化成凸优化过程，并提出L-BFGS优化算法求解该问题。同时他们还提出对抗样本在不同模型中具有迁移性（对抗样本可以导致不同深度学习模型分类错误）。2015年Goodfellow 等人提出线性假设证明了对抗样本的存在性，并提出了一种快速生产对抗样本的方法-快速梯度符号法（FastGradient Sign Method，FGSM）。同时他们提出利用该攻击方法进行对抗训练，可以提高深度学习模型的健壮性。2016年Carlini和 Wagner提出三种攻击方法，分别限制扰动，和范数使得扰动无法被深度学习模型察觉，同时该方法生成扰动可以在不同模型之间进行迁移，进而实现了黑盒攻击。2017年Kurakin 等人在原有的FGSM的基础上进行改进，将原有的单步生成对抗样本改进为迭代生成的方式，提出了(Basic Iterative Method，BIM)、最小可能类法 (Leastlikely Class Method，LCM)、迭代最小可能类法 (Iterative least-likely class method，ILCM) 等对抗样本生成方法，同时他们还发现被相机拍摄的对抗样本也会被深度学习模型错误分类，进而证明物理世界也存在对抗样本。2017年Madry 等人提出投影梯度法（Projected Gradient Descent，PGD）生成对抗样本，该方法在BIM方法上将初始攻击参数进行随机初始化，极大的提高了对抗样本的攻击性。2017 年，清华大学 TSAIL 团队 Dong 等人提出了动量迭代法 (Momentum Iterative Method，MIM)，该方法有着极高的黑盒攻击成功率。2018年AJ Bose等人提出一种基于生成对抗网络（Generative Adversarial Networks，GAN）攻击人脸识别系统的方法。

目前生成对抗样本方法的研究较为成熟，对抗样本的攻击从原有的简单针对于单张图像无目标白盒攻击，逐渐发展到目前的可迁移有目标黑盒攻击。对抗样本的扰动也变的越来越小。虽然现有的生成对抗样本的方法种类繁多，但大多方法是对FGSM和BIM的改进，又或者采用其他优化方法求解最小损失函数添加项方程。因此在研究如何防御对抗样本时，只需选取其中较有代表性的攻击方法即可。目前攻击效果较好的生成对抗样本方法有：BIM，PGD及Carlini and Wagner Attacks (简称C&W)。

### 1.2.2 对抗样本防御研究现状

目前针对对抗样本防御主要有三个方向：对输入图像进行预处理或修改模型训练过程，改进深度学习网络模型，辨别图像是否为对抗样本。本文根据以上三个方向简单介绍一些较有代表性的防御策略。

1. 对输入图像进行预处理或修改模型训练过程

蛮力训练：许多研究者发现在深度学习训练数据集中不断加入不同方法生成的对抗样本，可以不断的提高深度学习网络模型的健壮性。该方法需要大量的对抗样本，虽然在一定程度上可以正则化深度神经网络减轻模型过拟合，但Moosavi-Dezfooli指出无论添加多少对抗样本，都存在新的对抗样本能够欺骗网络。

数据压缩：2016年Dziugaite等人发现使用JPG对输入图像进行压缩可以减轻扰动对于模型的影响，但图像压缩同时会降低正常分类准确率。即使后来提出用PCA方法进行压缩，依旧无法解决该问题。

图像缩放：2017年Xie等人发现将输入图像进行随机缩放可以有效的降低对抗样本攻击强度。

图像重建：2019年jia等人发现对图像进行压缩重建能够有效的降低对抗样本的攻击强度。相比图像压缩，该方法对正常分类准确率影响较小。

1. 改进深度学习网络模型

深度压缩网络：研究者发现简单的将去噪自动编码器（Denoising Auto Encoders，DAE）堆叠到原有的网络中可以减轻对抗样本的攻击，但会使网络模型变得更加脆弱。因此Gu等人提出深度压缩网络（Deep Contractive Networks，DCN），该方法使用了类似于压缩自动编码器（Contractive Auto Encoders，CAE）平滑度惩罚项。

梯度正则化或梯度隐藏：研究者发现使用输入梯度正则化可以有效的提高深度学习网络模型的健壮性，并且该方法配合蛮力对抗训练可以取得非常好的防御效果，缺点是网络计算复杂度太高。

知识蒸馏：2016年Hinton提出将复杂网络的知识迁移到简单网络中，可以有效的抵抗小幅度对抗样本攻击。该防御方法被Carlini和 Wagner提出的攻击方法攻破。

Parseval 网络：2017年Cisse等人提出通过控制网络每一层的Lipschitz 常数，可以有效的减轻对抗样本的攻击。

1. 辨别图像是否为对抗样本

2017年Issaranon等人提出激活函数Relu对于普通图像和对抗样本输出模式不同，并提供了一种基于SVM区分图像是否为对抗样本的方法。2018年Hinton提出使用胶囊网络重构图像可以辨别图像是否为对抗样本。

虽然目前已有的对抗样本防御方法众多，但大多是减轻对抗样本的影响。随着生成对抗样本方法研究的不断深入，对抗样本的扰动变得越来越小，同时对抗攻击目标从原来的小数据集转变成自然数据集，这极大的增加我们设计对抗样本防御策略的难度。同时在设计对抗样本过程中不仅仅要考虑如何提高对抗样本分类准确率，还要考虑普通正常样本分类准确率和防御的训练成本。

## 1.3研究内容及章节安排

# 对抗样本攻防理论基础

### 2.1对抗样本的定义

2014年Szegedy等人首次提出对抗样本概念，他们发现深度神经网络很容易受到对抗样本的攻击。对抗样本只是在原始样本中添加轻微扰动，人眼甚至无法察觉这些扰动，就能使得分类器输出错误的结果。同时他们还对对抗样本有如下定义：

假设将图像映射为一组向量的深度神经网络分类器为：



其损失函数可以表示为：



对于一个样本并且，则对抗样本生成可以表示为一个有界优化问题：



由于优化公式（2-3）算法复杂度太高不易计算，并且条件可以转化为，因此他们将该问题进行优化，优化后的公式为：



对于公式（2-4）他们提出用L-BFGS优化算法去求解该问题。在求解对抗样本的同时，他们还发现对抗样本对于低纬度的隐藏层输出影响较小，对于高纬度隐藏层输出影响较大。最后他们对于对抗样本存在性问题，提出了一个可能的解释（如图2.1所示）：现实世界出现对抗样本的概率很低，因此训练集和测试集中几乎不存在对抗样本或者说训练集无法覆盖所有的样本，又因为深度神经网络的高度非线性，导致过拟合只学习到非对抗样本的特征，并没有学习到泛化性特征。

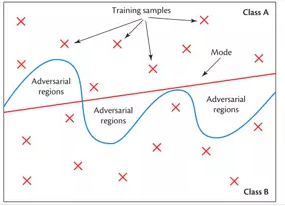


图2.1 深度神经网络模型训练与使用

如图2.1所示，蓝线为样本的真实决策边界，红线为模型训练得到的决策边界。可以从图中发现，模型训练后的最终决策边界和真实样本决策边界有较大的差别，这表明对抗样本是广泛存在的。

### 2.2生成对抗样本方法

在对抗样本概念被提出之后，越来多研究人员致力于改进生成对抗样本的方法。目前对抗样本攻击主要分为两类：一是白盒攻击，攻击者能够获取深度神经网络结构及参数，另一类是黑盒攻击，攻击者完全不知道深度神经网络网络结构及参数，只能通过模型输入获取输出。其中黑盒攻击可以通过对抗样本的迁移性来实现（用一个已知网络模型生产对抗样本，然后攻击未知模型），或者直接根据定义（只通过模型的输入输出）进行优化生成对抗样本，比如使用GAN生成对抗样本：生成器产生对抗样本扰动，未知深度神经网络分类器模型作为辨别器。虽然黑盒攻击和白盒攻击从攻击的目的来说有很大的不同，但其生成对抗样本的本质并没有区别。与黑盒攻击相比，白盒攻击攻击效果要更好，并且目前的黑盒攻击大多是白盒攻击的迁移或者融合多种白盒攻击。除此之外，对抗样本攻击是否具有目标性分为有目标攻击和无目标攻击。有目标攻击是指对抗样本能够使分类器以高置信度输出指定分类结果，无目标攻击只需使分类器输出错误结果即可。

由于生成对抗样本的方法众多，并且还在不断改进。因此本文选取目前较有代表性的三种生成对抗样本方法，简单介绍生成对抗样本的原理。

### 2.2.1快速梯度法-FGSM

2015年Goodfellow等人对生成对样本原因进行分析，他们发现扰动对深度神经网络影响会像雪球一样随着网络深度的增加越滚越大。由于神经网络的高度线性特性，导致这种效应相比非线性模型更加严重。基于深度神经网络高度线性及扰动“滚雪球”效应，他们提出了一种基于梯度的快速生成对抗样本方法FGSM，FGSM中对抗样本扰动计算公式如下：



其中表示模型输入，表示结果标签， 表示损失函数，表示符号函数，表示控制扰动大小的的自定义参数，表示生成的对抗样本扰动。FGSM算法的主要思想:如果扰动的方向和梯度方向一致，损失函数就会增大，进而使得分类器分类结果产生最大的变化。扰动越大损失函数就会越大，分类器结果产生的变化就会越大。

该方法可以通过一步快速生成对抗样本，并且该方法未直接使用梯度值而选择梯度方向有效的控制了对抗样本扰动的大小。虽然该方法生成速度快，使用的计算资源少，但使用该方法有诸多的限制。首先该方法适合白盒攻击，生成的对抗样本迁移性较差。其次该方法对于线性分类器模型攻击效果较好，对于非线性分类器模型和不可微分类器模型攻击效果较差。最后使用FGSM生成的对抗样本扰动较大（相当于每个像素点都增加了），该扰动自身抗干扰能力不强，容易受到其他噪声影响。

### 2.2.2基础迭代法-BIM

针对于FGSM存在的两个问题：损失函数与输入图像之间近似线性和扰动相较于原始图像改动较大。Goodfellow等人提出进一步的假设，如果损失函数与输入图像之间是非线性的，是否会存在一个存在于之间的某个扰动，使得变得更大。基于上述新的假设，Goodfellow等人提出了一种以迭代的方式生成对抗样本的方法BIM，生成对抗样本公式如下：



其中截断函数为：



截断函数的目的是保证的每一个像素都在的临域内且每个像素都有意义。BIM每次迭代的含义是：每次迭代在上一步生成的对抗样本基础上每个像素增加（也可能减少），然后对新生成的对抗样本进行裁剪，保证新的对抗样本每个像素都在的各像素临域内。BIM生成的对抗样本攻击效果一般要优于FGSM生成的对抗样本，最差的情况生成的对抗样本攻击效果与FGSM相同。

BIM生成的对抗样本攻击效果虽然优于FGSM，但由于其生成对抗样本迭代过程固定且每次迭代都是对上一次生成的对抗样本进行裁剪，这导致其能够迭代的次数较少，同时生成的对抗样本也容易受到其他噪声的影响。

### 2.2.3投影梯度法-PGD

2017年Aleksander等人发现采用PGD方式求解对抗样本中的优化问题效果要好于Goodfellow他们提出的使用梯度下降方式。PGD算法与梯度下降算法比较类似，都是用于求解非线性规划问题，但PGD算法在求解带有约束的非线性规划问题时具有更好的效果。PGD在求解对抗样本优化问题时，先选取一个可行解，然后将梯度下降的方向投影到约束集上，然后连接可行解点和梯度下降点生成可行的下降方向，最后重复上述过程直到对抗样本满足设定要求的精度。PGD生成对抗样本算法如下：



其中为一个学习步长，表示投影算子，该算子能将当前可行解投影到约束集中向量长度最小的向量上。PGD相较于BIM有更多的迭代轮次，并且往对抗样本中添加了随机化点，使得PGD的攻击效果远好于BIM。PGD生成的对抗样本也是目前一阶损失函数攻击攻击效果最好的算法。

### 2.3对抗样本防御策略

针对以上的对抗样本攻击特点，目前的防御手段主要有三个方向：对输入图像进行预处理，改进神经网络模型，检测输入是否为对抗样本。

对图像进行预处理：因为对抗样本是在原有的样本上添加而外的扰动噪声，一般情况下噪声越大攻击效果越好，同时因为目前深度神经网络高度线性特点扰动对神经网络影响主要是靠累加效应，因此只要减少对抗样本中的扰动就可以减轻对抗样本攻击效果。目前对图像的预处理主要是通过图像降噪，图像压缩，图像重建。图像预处理一定程度能减少样本中的对抗扰动，但是代价是会降低整个模型的分类精度。

改进神经网络模型： Szegedy等人提出对抗本概念时也指出对抗样本会导致神经网络高层输出远高于普通样本。根据以上特点Goodfellow等人提出使用Lipschitz常数来控制神经网络的层与层输出比例，进而防止高层神经元输出爆炸。Goodfellow等人在提出FGSM时也提出使用对抗训练能够很好的提高深度神经网络模型的健壮性。此外还可以通过提高深度神经网络模型非线性度来提高深度神经网络模型的健壮性。

检测输入是否为对抗样本：虽然对抗样本与原始样本相比变化十分微小，但神经网络对这两种样本输出特性完全不同，也有学者发现对抗样本无法用重构网络进行重构。因此我们可以通过另一个模型观察神经网络分类器输出特性来区分样本是否为对抗样本，或者使用胶囊重构来辨别输入是否为对抗样本。

本文将选取三种具体的防御策略，进一步分析各方向防御策略的优缺点。

### 2.3.1图像压缩重建

图像压缩重建防御策略属于图像预处理防御策略的一种，其主要思路：在图像进入分类器之前将图像“净化”，得到不包含对抗扰动的干净图像后再送入分类器中；图像“净化”主要利用了图像压缩过程去除冗余信息的思想，图像压缩后只保留了主要信息，对抗样本扰动属于冗余信息，图像压缩重建后这部分冗余信息将被去除；同时压缩重建模型和分类器分开训练，并不会影响到已经训练好的模型。图像压缩重建模型图2.1所示：

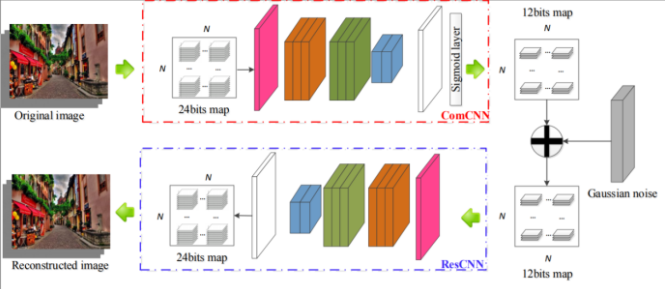


图2.1 图像压缩重建网络结构

图像压缩重建防御策略主要的优点是：不需要专门训练对抗样本，因为未改变分类器模型所以不需要重新训练分类器模型，“净化”后的图像在不同的分类器模型中都有较高的分类准确率。主要缺点是图像在经过压缩重建后图像质量会下降，这会导致分类器对无噪声图像分类准确率下降。

### 2.3.2对抗训练

对抗训练是指在分类器损失函数中添加一个正则项，该正则项是基于对抗样本引发损失的建模。分类器模型使用这种新的损失函数进行训练可以提高模型对对抗样本的泛化能力。实际操作是在原始模型训练集中添加对抗样本，进而提升模型对于对抗样本扰动的健壮性。使用FGSM作为对抗训练模型损失函数修改如下：



其中为模型原始损失函数，表示对抗样本引发的损失。对抗训练的好处是模型可以防御已知的对抗样本生成方法生成的对抗样本（只需向模型训练集中添加足够的该对抗样本生成方法生成的对抗样本），并且防御效果很好。缺点也很明显，对于新种类的对抗样本没有防御能力，并且每出现一种新的生成对抗样本方法，要想防御必须将该生成对抗样本生成的对抗样本加入到模型的训练集中然后重新训练，反复重新训练模型极大的提高了实施防御的成本。

### 2.3.3通过胶囊网络检测对抗样本

Frosst等人提出只需简单的改进胶囊网络训练方式就能使胶囊网络检测出对抗样本图像。他们除了正常训练图像分类任务之外，还训练胶囊网络根据顶层的姿态参数来重构原始图像。因为对抗样本与分类器分类结果类有较大的不同，所以会导致通过该类的顶层胶囊重构图像时会有较大的重构误差（图2.2给出了从真实数据和对抗样本生成的重构图像）。他们通过实验证明在输入图像和重构图像之间的距离上设置阈值可以有效的检测出对抗样本。

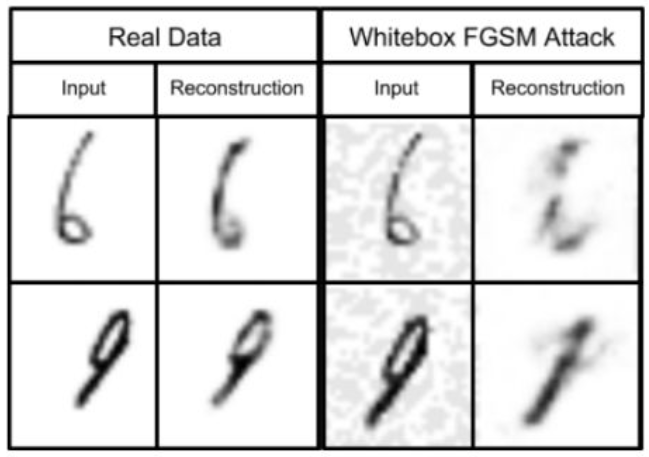


图2.2 真实数据与对抗样本生成的重构图像

该检测对抗样本方法主要适用于较小的数据集（如MNINST），在更复杂的数据（如Cifar-10和ImageNet）中两张图像看起来相似，但距离很大，这导致该方法并不能检测出图像是否为对抗样本。另外作者还发现该方法无法检测出强对抗攻击，此类攻击在可视化结果中，被干扰的图像与目标类的数据流十分相似。

### 2.4对抗样本攻防总结

虽然目前有许多的生成对抗样本方法，同时不同生成对抗样本方法攻击的目标也不同，但对抗样本的特征是基本相同的，目前对抗样本主要特点有：对抗样本存在并不唯一，对抗样本攻击可以是有目标的也可以是无目标的；对抗样本具有迁移性，但对抗样本在用于未知模型时其攻击效果会降低；虽然生成对抗样本方法众多，但其本质是一样的，且目前的生成对抗样本算法大多是对FGSM算法进行改进；使用同一种生成对抗样本算法生成的对抗样本，对抗样本扰动越大其攻击效果越强同时抗干扰能力也越强；深度神经网络对于对抗样本与普通样本输出特性完全不同，这说明对抗样本与普通样本可能有着不一样的分布。

目前的防御策略主要存在三个问题：一是大部分防御策略是削弱对抗样本对神经网络模型的影响，二是许多防御策略需要重新训练分类器模型这导致防御成本极高，三是大部分防御策略会导致无噪声图像分类准确率下降。因此在制定对抗样本防御策略时不仅要考虑防御效果还要考虑防御成本及是否会影响普通样本分类准确率，由于现实生活中对抗样本存在的可能性较小，因此制定防御策略时要着重考虑是否会影响普通样本的分类准确率。如果防御策略能够在不同模型之间迁移，可以有效的减少防御成本。

# 基于VAE-GAN的对抗样本防御策略

目前已有的对抗样本扰动大多十分微小（人眼难以察觉），然而深度神经网络模型对这些扰动十分敏感。目前许多防御手段目的是消除对抗样本中的扰动，使其恢复成原本的图像，这些方法对于部分扰动较大的对抗样本十分有效。但清华大学 TSAIL 团队 Dong 等人发现即使除去对抗样本的大部分噪声，部分攻击性强的对抗样本依然能够影响深度神经网络模型，使其输出错误的分类结果。Issaranon等人发现虽然对抗样本与原始样本十分相近，但深度神经网络模型对于两种样本输出特性完全不同，这表示对抗样本与原始样本的分布可能是不一样的。基于对抗样本以上两点特性，本文提出一种新的防御策略——基于VAE-GAN的对抗样本防御策略，VAE用于对图像的压缩重构以去除对抗样本中的扰动，GAN用于辅助VAE中的解码器使其重构出的图像与无噪声图像分布相同，同时提高重构生成图像的图像质量，保证无噪声图像经过压缩重构后图像质量。

## 3.1基于VAE-GAN防御策略整体框架

变分自动编码器（Variational Auto-Encoders，VAE）模型是一种基于变分贝叶斯推断的自监督类深度学习模型，主要用于数据压缩，图像降噪等方面。VAE主要由两个部分组成：一为编码器（encoder）能够将原始输入数据生成隐变量的变分概率分布，另一个为解码器（decoder）能够将隐变量的变分概率分布还原成原始输入数据。VAE结果示意图如图2所示：

VAE与传统的自动编码（Auto-Encoders，AE）特性完全不同，VAE的隐藏空间被设计成连续分布目的是更好的随机采样和插值，这使得VAE相较AE为更有效的生成模型。VAE通过独特的方法来实现上述特性，VAE的编码器先输出两个维矢量：分别为均值向量和标准差向量。使用这种随机生成的方式即使对于相同的均值和方差，实际的编码也会因为每一次采样不同产生不同的编码结果。其中均值向量用于控制编码的输入中心，标准差用于控制编码相对均值变化的范围。通过这种采样方式得到的编码可以是连续分布区域范围内的任意一点，解码器学习到的不是一个单点在隐藏空间的中的表示而是整个领域范围内点的编码表示。解码器通过一定程度变化编码训练而成，这使得解码器不仅能够解码隐藏空间中的单一特征点，还可以解码该特征点一定领域范围内的编码。

VAE的编码器的输出和解码器的输入都受均值向量和标准差向量的维正态分布影响，而我们