

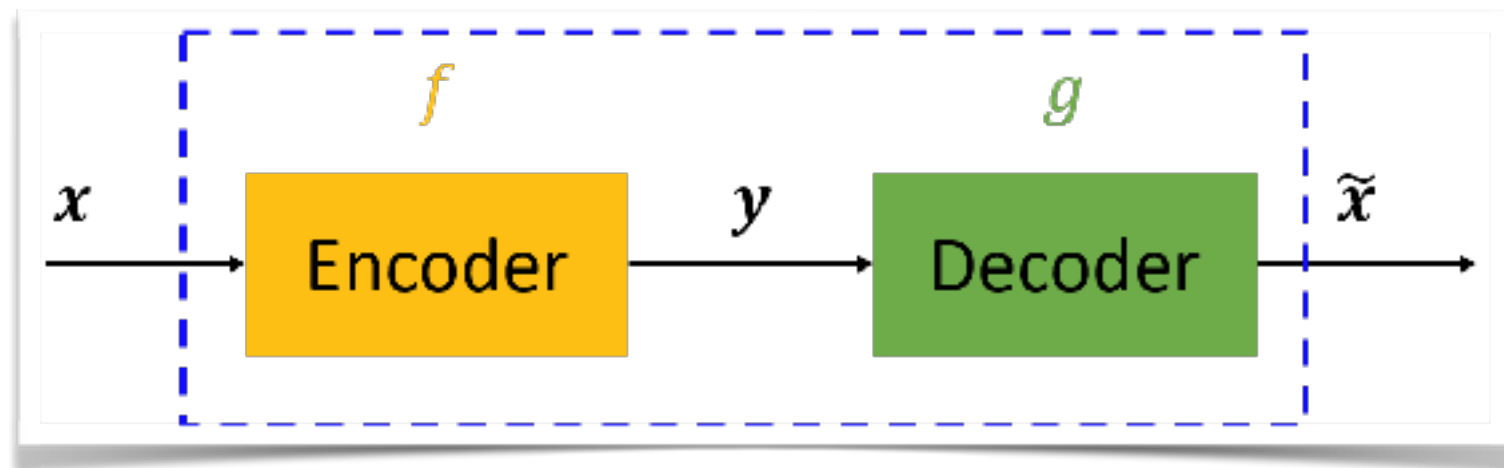
# 深度学习

自编码器

# 基本概念

**自编码器(Autoencoder, AE)**往往也称为自编码算法。它是神经网络的一种，它尝试逼近一个恒等函数，从而使神经网络的输出 $h$ 接近于输入 $x$ 。即自编码器是一种转换数据表现形式的算法。严格的来讲自编码器不包括神经网络的输出层。自编码器是无监督学习算法。

# 编解码器



我们希望编码器能够对数据进行编制、转换。解码器能够对数据进行还原。

自编码器类似于编解码器中的编码器

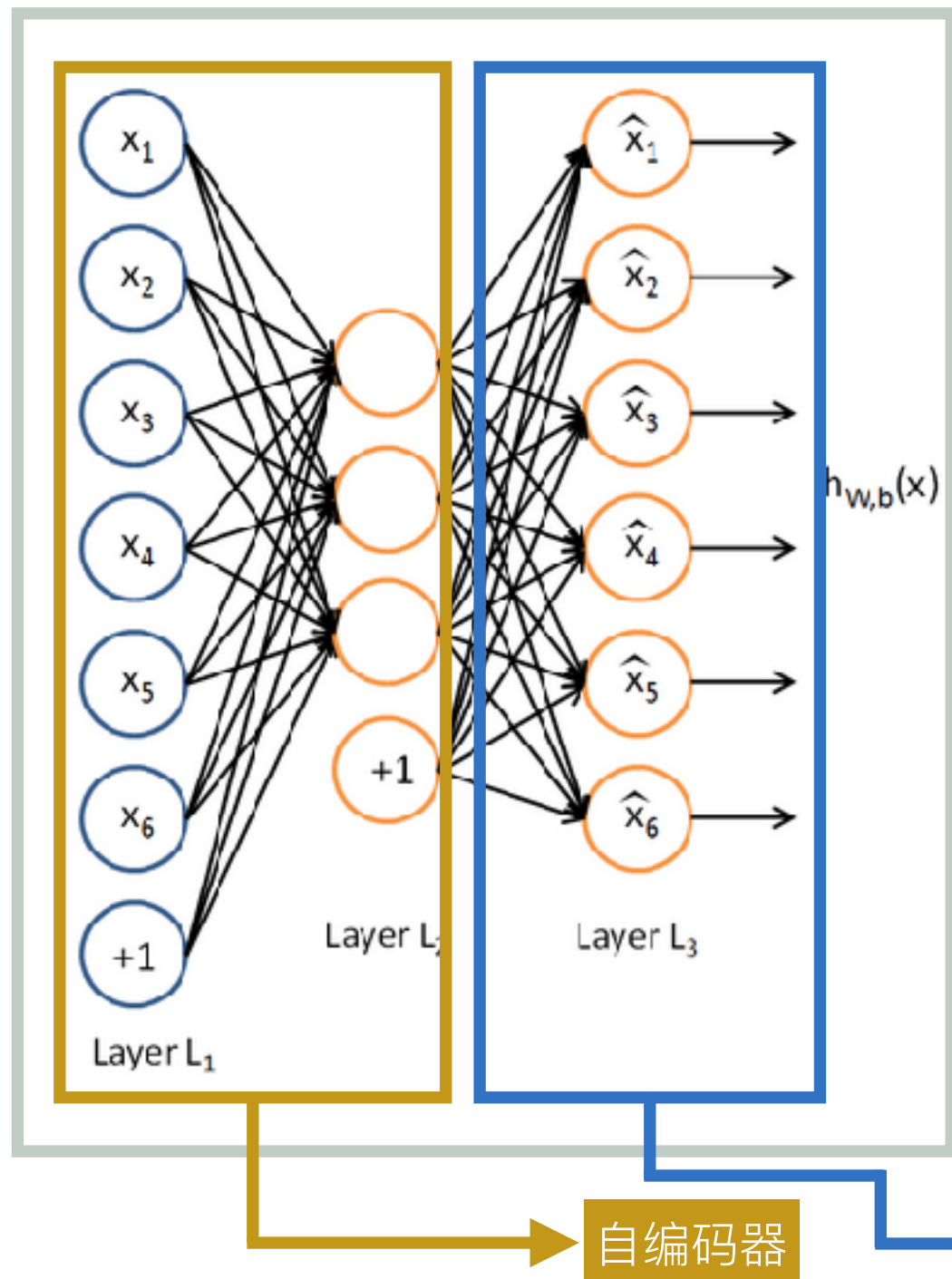
注意：此处使用的变量符号与神经网络中的符号不是对应关系！

$$y = f(x)$$
$$\hat{x} = g(y) = g(f(x))$$

# 思考：编解码器中的 $f$ 与 $g$ 是恒等映射吗？如果不是恒等映射会产生什么结果？

如果是恒等映射，则可以完全还原数据，即 $f$ 输出的中间结果包含了全部原始信息。如果 $f$ 与 $g$ 不是恒等映射，则相当于 $f$ 输出的中间结果是原始数据的另一种表达形式，但不一定包含了全部的原始信息。

# 自编码解码器



自编码解码器是3层神经网络

输入层与输出层神经元数量相等

隐藏层往往与输入层神经元数量不相等

自编码解码器的输出近似等于输入

自编码解码算法(自编码算法)

自编码器

解码器

# 自编码解码器

代价函数

$$J(x, \hat{x}) = \frac{1}{m} \sum_{i=1}^m \|x^{(i)} - \hat{x}^{(i)}\|^2$$

意义

通过梯度下降法训练自编码解码器，当训练结束后，这个网络即学习出了 $x \rightarrow a \rightarrow x$ 的能力。对我们来说 $a$ 是至关重要，因为他是在尽量不损失信息量的情况下，对原始数据的另一种表达。

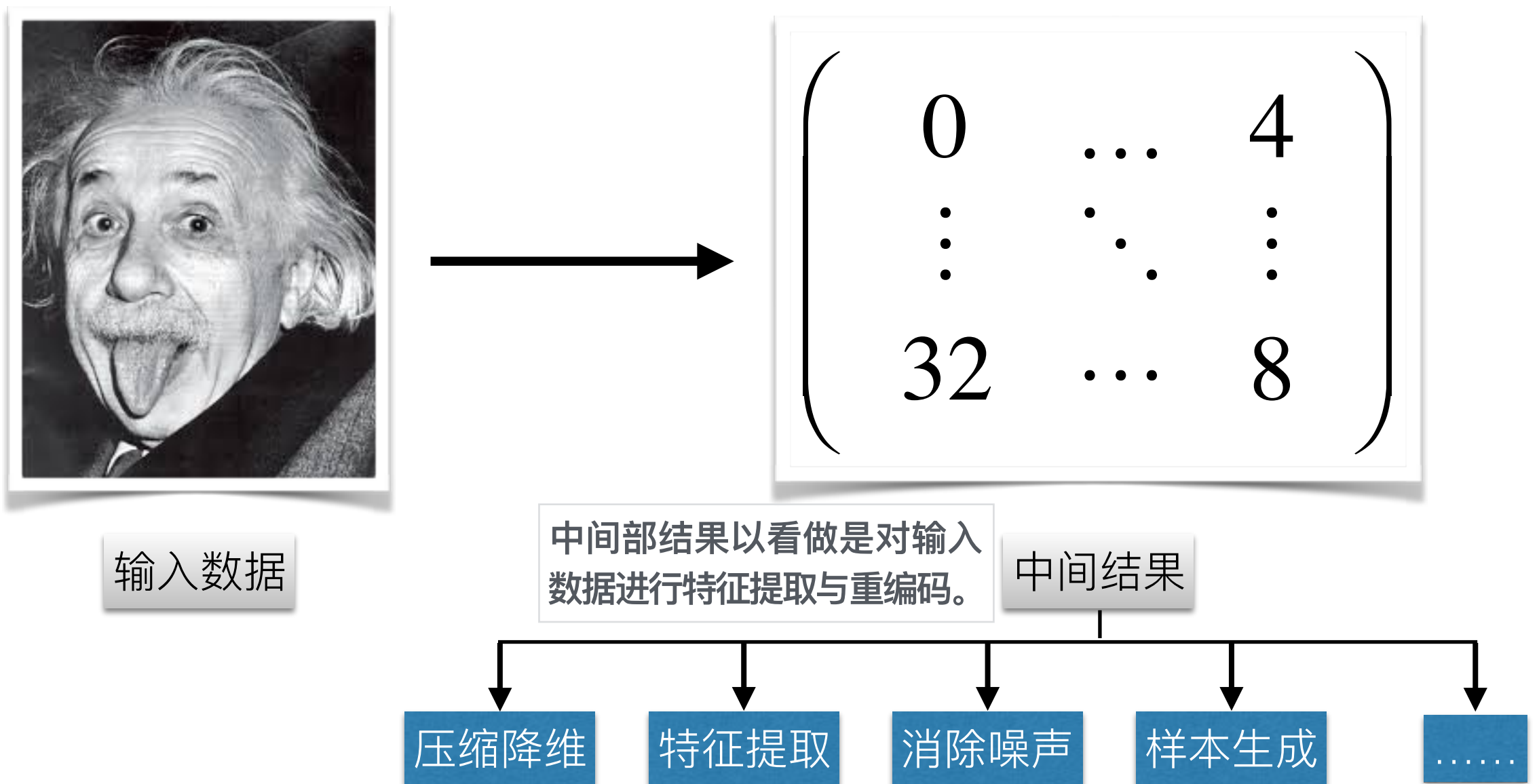
思考1：代价函数使用对数似然函数可以吗？

不可以

思考2：数据的另一种表达形式有什么意义？

# 自编码器

自编码解码器中最重要的部分就是隐藏层。输出层仅仅是为了衡量隐藏层是否学习到了规律。



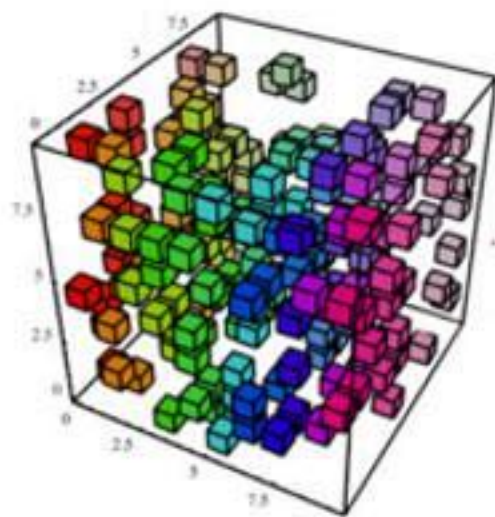
# 自编码器的种类

- 自编码器。普通的自编码器，通常其隐藏层单元数量小于输入层单元数量。可用于数据降维。
- 稀疏自编码器。通过对隐藏层添加稀疏性约束使神经元的平均激活度降到较低。可用作特征提取与表达。
- 降噪自编码器。通过巧妙的训练方法，使自编码器拥有降噪的能力。可用作数据降噪。
- .....

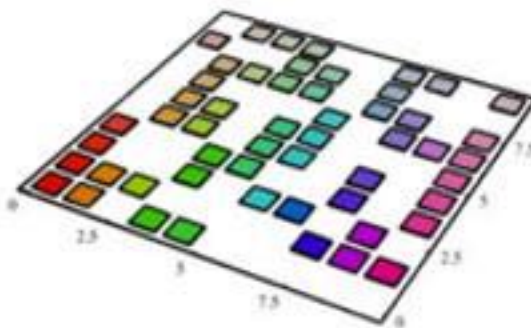


# 自编码器用于降维

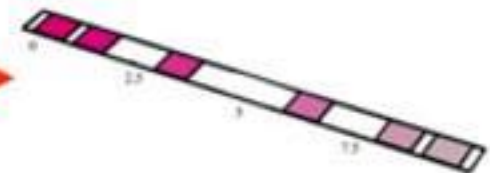
降维是指在某些限定条件下，降低随机变量个数，得到一组“不相关”主变量的过程。



3 dimensions: 1000 positions!

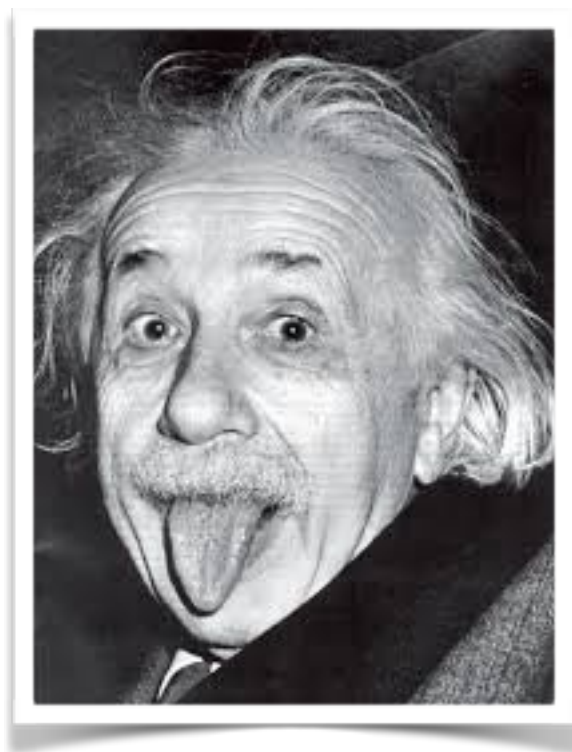


2 dimensions: 100 positions



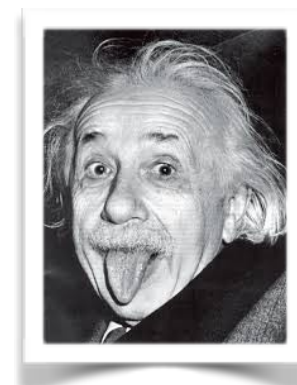
1 dimension: 10 positions

# 小练习



180px\*240px

降维



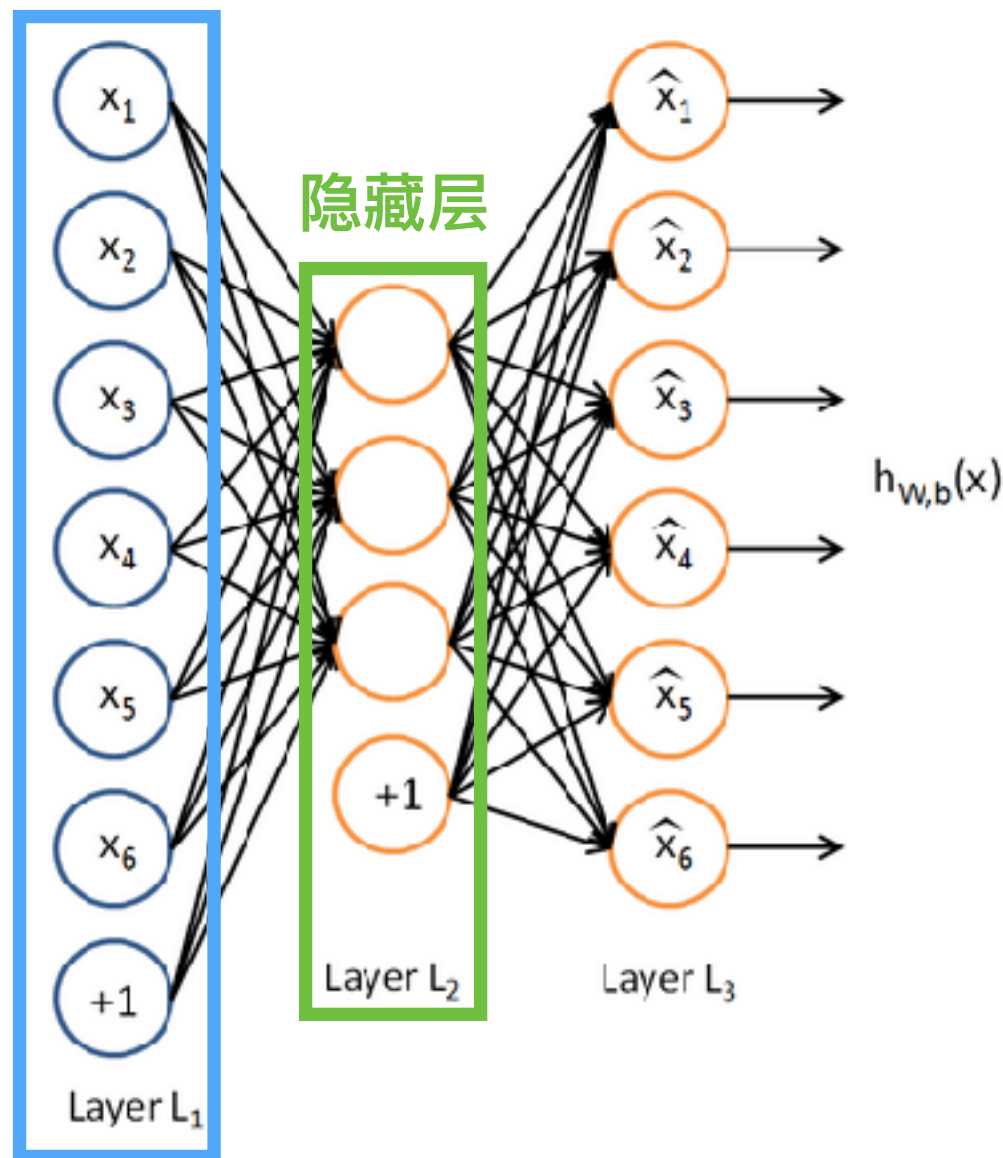
90px\*120px

将图片缩小的过程是降维吗？

不是

# 自编码器用于降维

输入层



使隐藏层神经元数量小于输入层神经元数量。然后训练神经网络，使输出尽量还原输入。训练的过程就是降低错误的过程，为了达到这一目的，隐藏层必须要以更少的单元尽量表达更多的信息。



隐藏层神经元学习到了输入数据中的特征与特征表达方法。

# 小练习

训练得到的自编码器（自编码器不包括输出层）只有与之相连的输出层以及相关参数才能够解码利用数据吗？

与隐藏层相连的输出层以及相关参数相当于自编码器的解码器。但并非只有训练时的输出层以及相关参数才能对数据进行解码。因为隐藏层的输出代表的是原始数据的另一种表达形式，其蕴含了原始数据的绝大部分有效信息。对于我们来讲，无论是原始数据还是隐藏层输出的中间结果，均蕴含了等价的信息，均可以被其它算法利用。只是使用的场景与方法不完全相同。

# 自编码器用于降维

**方法：使隐藏层神经元数量小于输入层神经元数量。**

**目标：在允许的误差率下减少隐藏层神经元的数量。**

**意义：网络试图以更小的维度去描述原始数据而尽量不损失数据信息。当每两层之间的变换均为线性，且训练使用的是均方误差代价函数时，该网络等价于PCA。**

# 为什么数据能够降维

- 自然界的规律是有规律的。即可以从原始信息中提取到特征。
- 自然界的规律所蕴含的特征是稀疏的。同时输入的有效信息有冗余。
- 信息中可能含有无用的噪声数据。



## 举例：

人脸识别任务中，我们需要输入一张人脸照片。

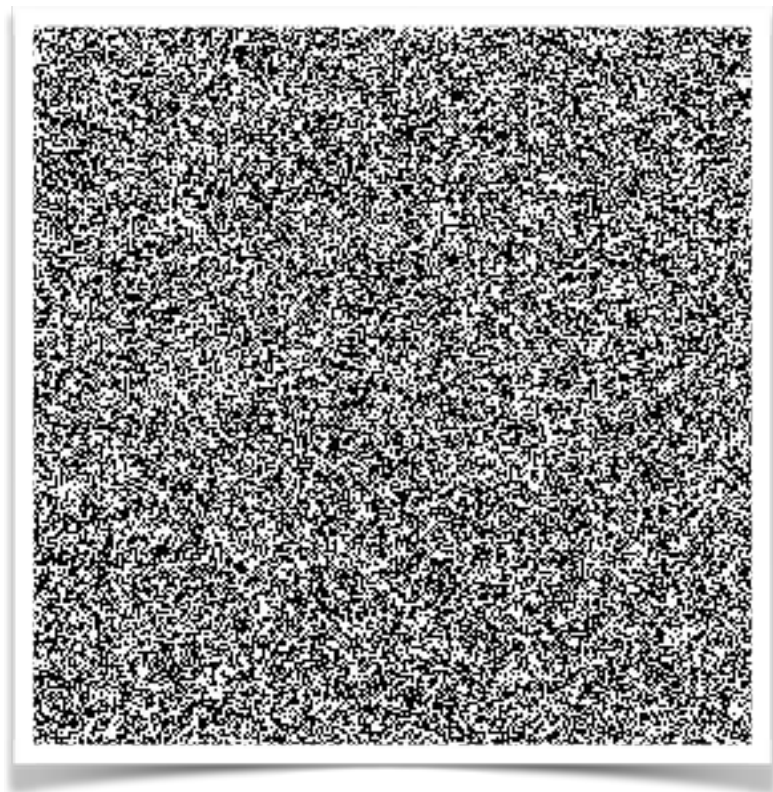
绿色的背景  
是噪声数据



眼睛的像素组合方式  
是固定的。可以看做一个宏观特征。

肤色是冗余信息

# 思考：使用噪声图片输入降维自编码器会发生什么？



通过训练代价几乎甚至根本无法降低。

隐藏层对输入数据的转换是无效的。

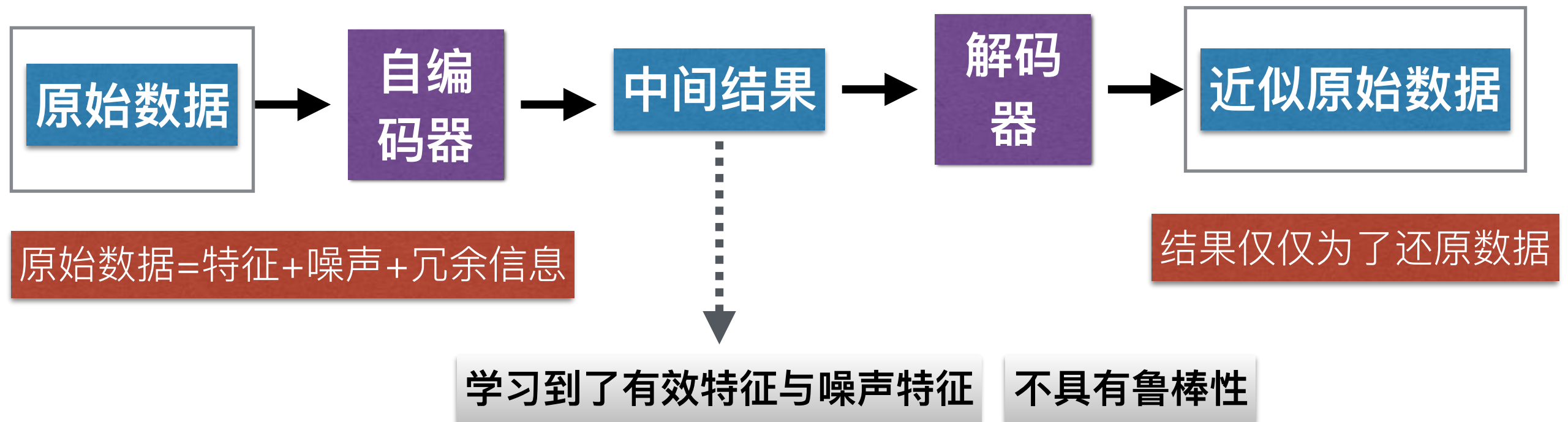
**自编码器失效**

**自编码器只能对包含信息的有效数据就行处理。**



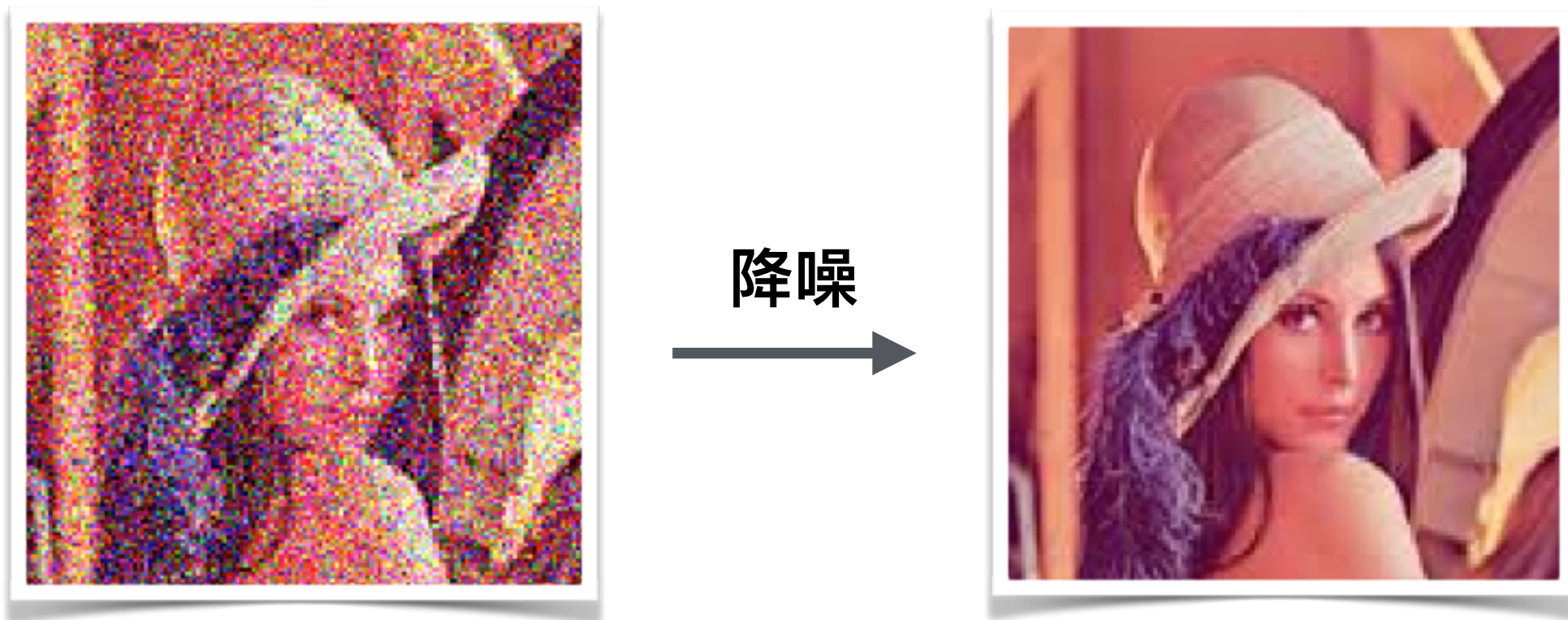
# 自编码器与鲁棒性

鲁棒性：指系统在扰动或不确定的情况下仍能保持它们的特征行为。鲁棒性也称为健壮性。

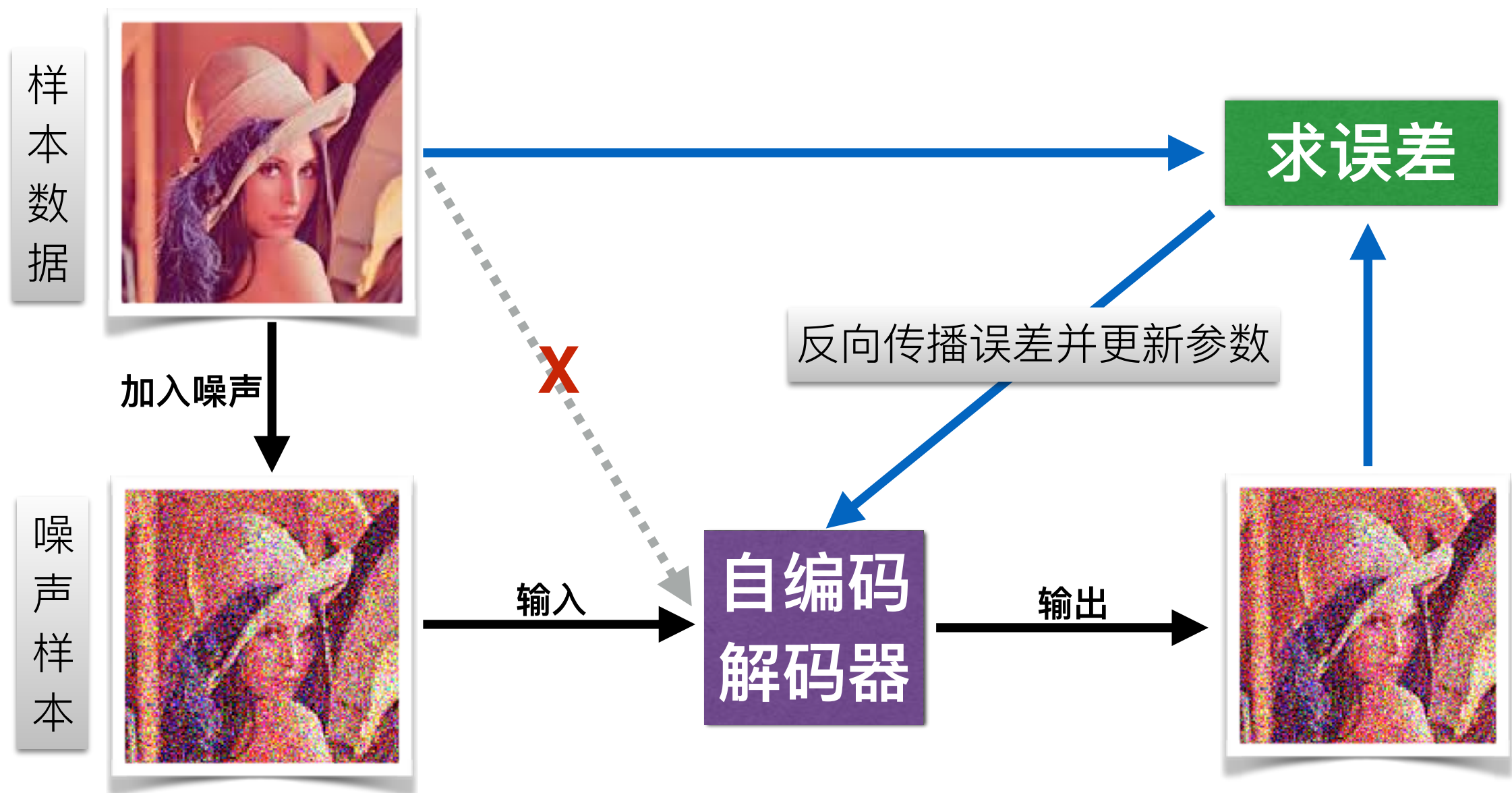


# 自编码器用于降噪

自编码器可以用于对输入数据进行降噪，即还原数据中丢失的信息，去掉数据中的干扰，我们称这种自编码器为降噪自编码器(Denoising AE)。



# 自编码器用于降噪



# 降噪自编码器

## 方法

给输入数据加入噪声。并使用原始数据训练神经网络。

## 目的

消除噪声，还原原始数据。

## 作用

对抗噪声。增强对新数据的适应能力。

我们使用 $\tilde{x}$ 表示加入噪声的输入,  $\tilde{x} = f(x)$ 。则代价函数为

$$J = \frac{1}{m} \sum_{i=1}^m ||x^{(i)} - h(\tilde{x}^{(i)})||^2$$



## 思考：为什么降噪自编码器能够去除噪声并还原数据？

1. 使用原始数据与生成结果做误差可以告诉神经网络丢失的信息是什么。以此来找到丢失信息与输入信息的关联。
2. 部分特征信息是冗余的。丢失一部分不影响这些特征的完整性。
3. 特征的独立性可以使得神经网络重构部分丢失的特征。

# 思考：为什么自编码器均为3层？

1. 避免深层神经网络因梯度消失导致其难以训练的问题。
2. 自编码器可以堆叠成多层。我们称之为栈式自编码器。

# 小结

- 自编码器是一种三层神经网络训练后得到的结果。严格来讲自编码器不包括输出层。自编码器算法指三层神经网络的结构以及其训练算法。
- 自然界的信息表达往往是冗余的、稀疏的。
- 降维自编码器的关键是使隐藏层的单元数量少于输入层的单元数量。
- 降噪自编码器的关键是利用加入噪声的数据正向传播，利用原始数据计算代价。通过训练可以指明噪声，还原数据。

# THANKS