生成对抗网络驱动的图像隐写和水印模型

作者：郑钢，胡东辉，戈辉，郑淑丽 时间：2021

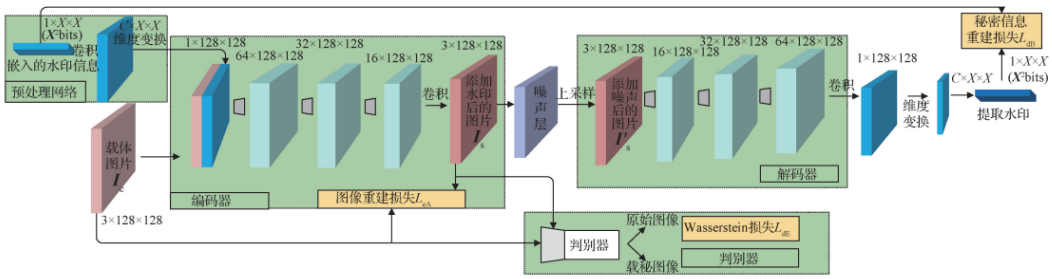
期刊：中国图像图形学报 第26卷第10期

前言

- 图像信息隐藏技术包括有隐写术和图像水印技术两种，研究者们试图利用生成对抗网络进行自动化的隐写算法以及鲁棒水印算法的设计，但所设计的算法在信息提取准确率、嵌入容量和隐写安全性或水印鲁棒性、水印图像质量等方面存在不足
- 该文提出了基于生成对抗网络的的新型端到端鲁棒水印模型，网络模型中使用了更有效的编码器和解码器结构SE-Resnet，该模块根据通道之间的相互依赖性来自适应地重新校准通道方式的特征响应。实验结果显示水印模型在提升水印嵌入容量的同时显著提升了水印图像质量以及水印提取正确率，在JEPG压缩的攻击下较对比方法提取正确率提高了约20%
- 该文的水印模型的主要贡献为：
    - 提出了一个使用SE-ResNet模块的更有效的编码器和解码器结构，SE-Resnet模块可以通过显示地建模通道之间的相互依赖性来自适应地重新校准通道方式的特征响应。因此，秘密信息可以被隐藏到图像中并被更完美地提取，从而提高了编码图像的感知质量以及信息提取准确率。
    - 对于基于生成对抗网络的鲁棒盲水印模型 在噪声层中考虑了丰富多样的噪声类型以及高强度的噪声攻击,对于不可微分的 JPEG 压缩操作,本文 提出了一种更有效的模拟方法。

IRBW-GAN模型：

-



(b) IRBW-GAN

- 编码器：收到形状为3x128x128的载体图像Ic和形状大小为1xXxX（X²bits水印信息），在编码器之前，有一个预处理网络层，目的是为了将初始的水印信息进行变换，增加其冗余空间。在编码器和解码器之间是一个噪声层，通过将各种噪声建模成可微分的网络层来训练抵抗各种噪声攻击的鲁棒水印。解码器：接收到添加噪声后的图片Ia'并提取嵌入其中的信息，判别器用于判别图像是载体图像还是嵌入水印的图像，并且在判别器中使用W-GAN-gradient penalty的损失函数以稳定训练过程。
- 编码器和解码器的结构：
    - 在编码器和解码器网络中使用了3个SE-Resnet模块，以将秘密信息自动嵌入到载体图像难以检测的区域中，并有效地提取信息。对于编码器网络，每个块的卷积内核数增加2倍，而解码器网络则相反。在整个编码器和解码器中没有使用任何池化层，从而最大程度地减少了信息丢失。卷积核的尺寸为3x3，步幅为1，填充为1。该卷积方法确保最大程度不丢失载体图像的固有信息，从而确保由编码器生成的图像质量，并使解码器最大程度的准确提取信息。

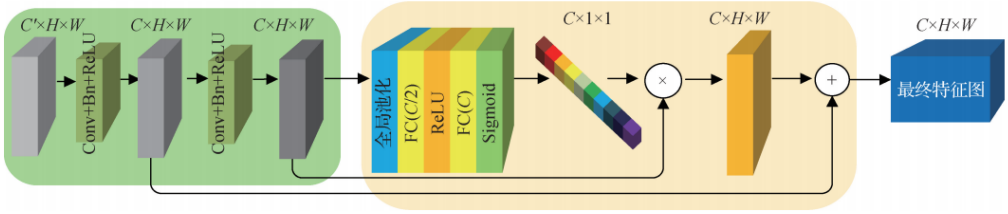
- 

图 2　SE-ResNet 模块详细结构

- 判别器的详细结构：

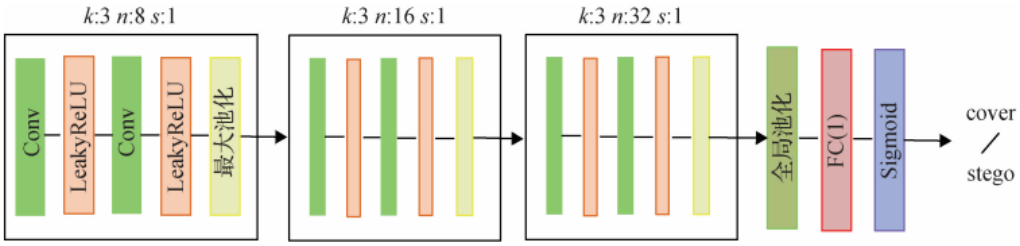


图 3　判别器详细结构

- 噪声层：
  - 噪声类型说明

表 1　噪声类型说明

Table 1　The description of the noise type

噪声类型	具体含义
Identity	恒等噪声
Dropout	Dropout 噪声
Cropout	Cropout 噪声
Crop	裁剪噪声
JPEG compression	JPEG 压缩噪声
Resize	缩放噪声
Mean filtering	均值滤波噪声
Gaussian blur	高斯模糊噪声
Salt & Pepper	椒盐噪声

  - 恒等噪声：即在噪声层中不对水印图像进行任何处理，相当于水印图像没有经过任何处理直接输入到解码器中，这是用于与各种噪声攻击类型进行对照实验的。
  - Dropout 和 Cropout 都有一个强度因子p（0~1）
  - Crop 和 Resize 分别表示裁剪和缩放操作各有一个强度因子p ,表示的是裁剪 和缩放之后的图像与原图大小比例为p 。
  - Mean filtering 表示均值滤波,会导致图像模糊, 常用于图像去噪。 使用 3 × 3 均值滤波器对原始图像进行卷积操作即可得到噪声图像。

结论

- 该文提出了一个图像鲁棒盲水印模型IRBW-GAN。通过设计基于SE-Resnet块的编码器和解码器，实现了更加准确、高质量的信息嵌入和提取；通过判别器与编码器-解码器的对抗训练，保持载体图像的分布不改变，并提高隐写对抗安全性。在水印模型中，本文在噪声层中考虑了丰富多样的噪声类型，并设计实现了一种新型的JPEG压缩模拟方法。

缺点：

- 对于水印模型来说,仍需提升对诸如裁剪操作的鲁棒性。 本文设计的鲁棒水印需要事先对噪声进行建模，但是现实生活中，可能存在的噪声类型是多种多样的，往往并不知道所有可能的攻击类型，而且很多噪声难以建模，很难转换成可微分的网络层，例如 JPEG 压缩。 因此，需要进一步考虑开发一种无须事先得知特定噪声类型，也能够鲁棒解码的图像水印技术，这更具有现实意义。