

# 图像信息隐写相关论文一

原创

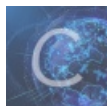
ningchewinbell 于 2020-04-09 18:56:39 发布 1426 收藏 10

分类专栏: [图像](#) 文章标签: [深度学习](#) [计算机视觉](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/ningchewinbell/article/details/105405122>

版权



[图像](#) 专栏收录该内容

8 篇文章 2 订阅

订阅专栏

[ste-GAN-ography: Generating Steganographic Images via Adversarial Training](#)

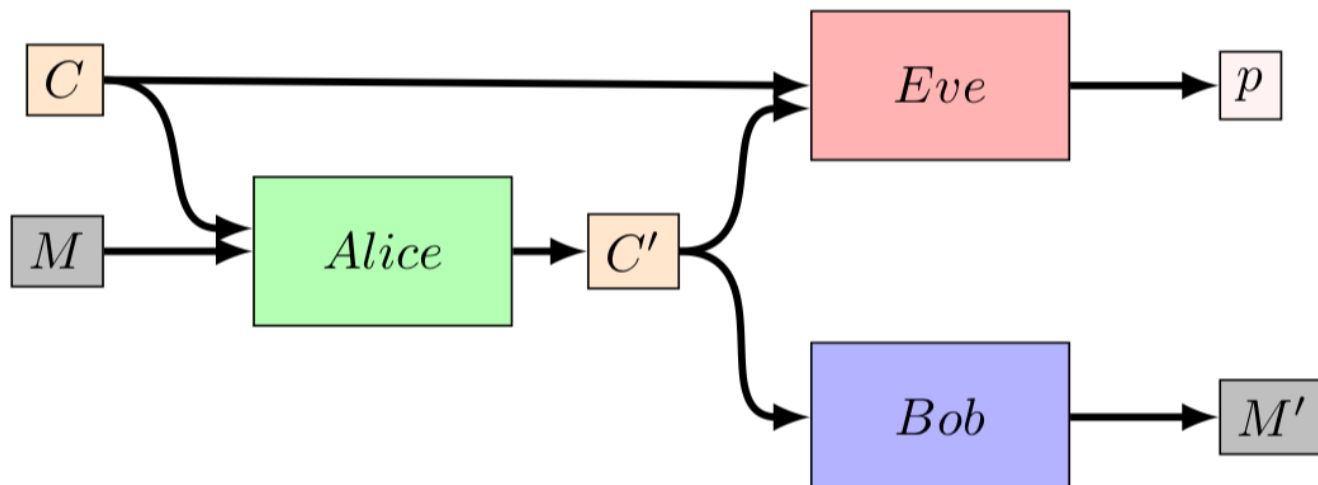


Figure 1. Diagram of the training game.

<https://blog.csdn.net/ningchewinbell>

这篇文章还是比较简单的, 模型主要包括三个子网络, 代表Alice、Bob和Eve三方, 如上图所示, Alice将秘密信息隐写在图像中传送给Bob, Bob要从收到了图像中提取出秘密信息, Eve窃取了图像并试图分析图像中是否包含秘密信息。

通过训练Alice可以有效地将秘密信息嵌入图像中, 作者通过实验与HUGO、WOW和S-UNWARD等隐写算法进行了比较。评估指标主要是ATS (当时性能很好的隐写分析算法《Unsupervised steganalysis based on artificial training sets.》), Eve。

(0.4bpp 0.4bit per pixel)

**Table 1:** Accuracy of distinguishing between cover and steganographic images for the steganalyzers, Eve and ATS, on the BOSS dataset at an embedding rate of 0.4bpp.

STEGANOGRAPHIC ALGORITHM	STEGANALYZER	
	ATS	EVE
ALICE	0.97	0.88
HUGO	0.87	0.90
WOW	0.94	0.93
S-UNIWARD	0.95	0.91

<https://blog.csdn.net/ningchewinbell>

文章的描述和我理解的有点不一样，如果表中是ATS和Eve的分辨是否隐写了秘密信息的准确率，那么应该是值越大性能越好，所以ATS比Eve更好，但是文章说的是Eve效果更好。不解...

#### Steganographic Generative Adversarial Networks

文章的目的是通过对抗学习生成更适合作为cover的图像（based on DCGAN）。模型图如下：

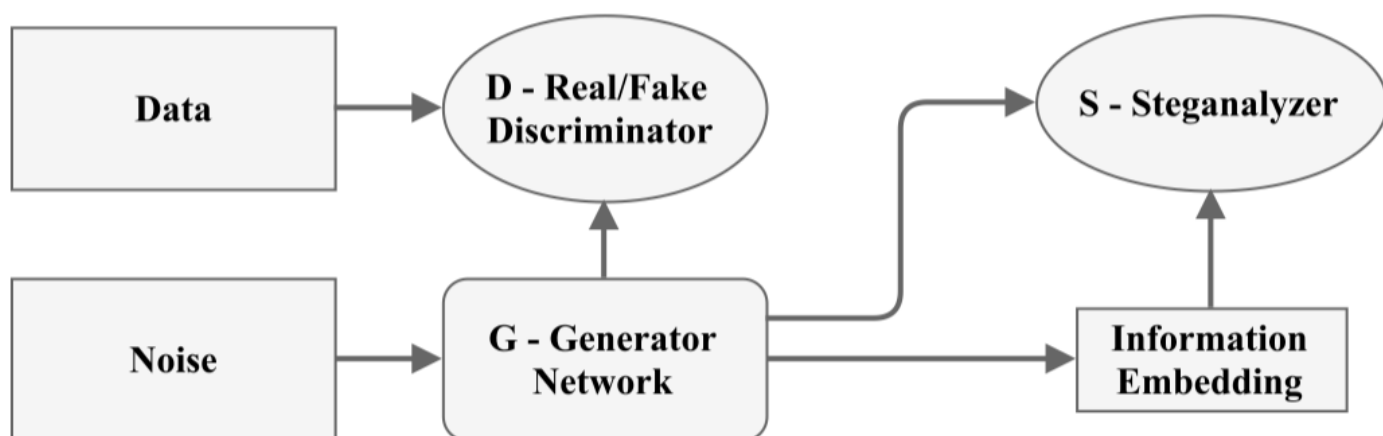


Figure 1: SGAN information flow diagram

<https://blog.csdn.net/ningchewinbell>

Steganographic Generative Adversarial Networks model (SGAN) 主要有三部分组成：

生成器G，生成看起来更真实的图像、

判别器D，判别是真实图像还是生成图像、

判别器S，判别图像中是否嵌入了秘密信息。

使用的嵌入方法为正负1-embedding algorithm。

Table 1: Accuracy of the steganalyser  $S^*$  trained on real images

Type of a test set \ Image generator	SGANs	DCGANs
Real images	0.962	
Generated images	0.501	0.522

<https://blog.csdn.net/ningchewinbell>

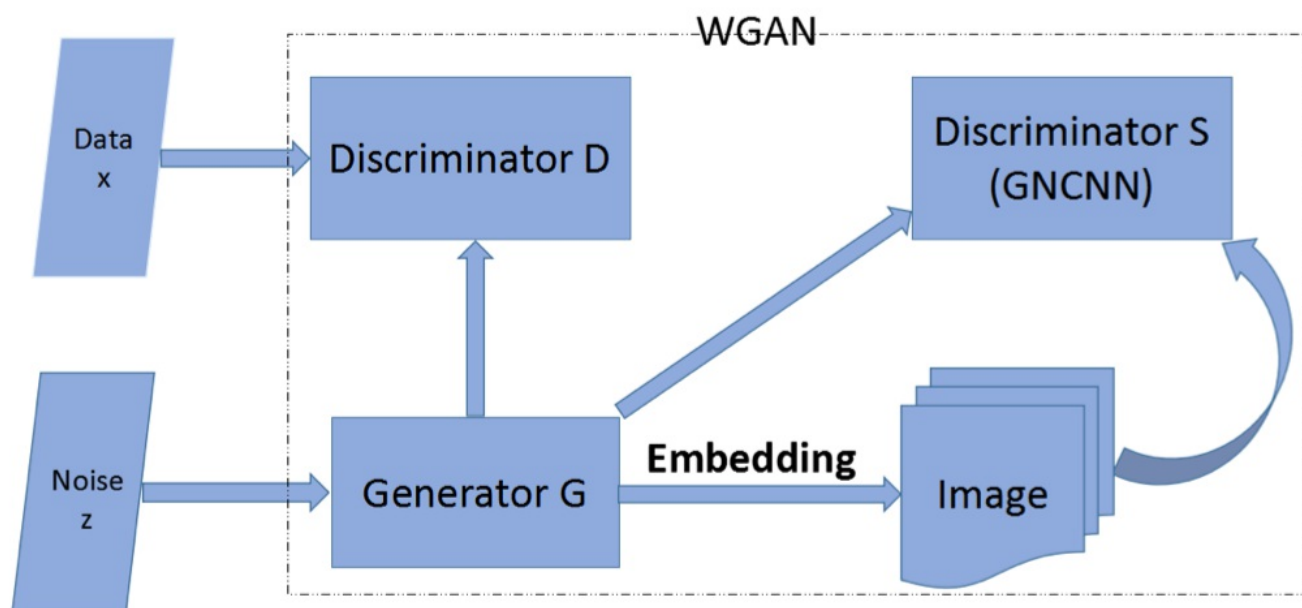
除了模型里的S外，独立训练了一个隐写分析器 $S^*$ ，用于评估生成图像的抗分析能力。对于真实图像训练得到的 $S^*$ ，不管是DCGAN还是SGAN生成的图像， $S^*$ 都几乎不能分辨出是否包含隐写信息。

未来将来将进一步用HUGO[Using High-Dimensional Image Models to Perform Highly Undetectable

Steganography.]、WOW[Designing steganographic distortion using directional filters.]和S-UNIWARD[Universal distortion function for steganography in an arbitrary domain.]作为隐写算法来测试我们的方法。

**SSGAN: Secure Steganography Based on Generative Adversarial Networks**

这篇文章和上一篇很相似，都是想通过对抗训练得到更适合隐写秘密信息的图像。除了模型里的S外（GNCNN: *Deep learning for steganalysis via convolutional neural networks*），独立训练了一个隐写分析器S\*，用于评估生成图像的抗分析能力。



**Fig. 1.** The SSGAN model

<https://blog.csdn.net/ningchewinbell>

不同点在于

- 1.用wgan代替了drgan
- 2.使用gncnn作为判别器S