

神经网络语言模型的性能优化研究

On Optimization Perspective of Neural Language Model

姜楠 (*nanjiang@buaa.edu.cn*)

北京航空航天大学计算机学院研究生开题答辩

2016 年 12 月 20 日



概览

- 1 论文选题的背景与意义**
- 2 国内外研究现状及发展动态**
 - 隐写分析
- 3 论文的研究内容及拟采取的技术方案**
 - 拟采取的技术方案
 - 论文的研究内容
- 4 论文研究计划**



题目来源

论文题目《神经网络语言模型的性能优化研究》为自拟课题。

题目来源

论文题目《神经网络语言模型的性能优化研究》为自拟课题。

LSB 隐写术 (LSB Steganography)

- 最早接触隐写术的概念在《密码学》课堂上
- 因为感兴趣曾经使用 Wolfram Mathematica 实现了基本的隐写程序，并写入了博客

题目来源

论文题目《神经网络语言模型的性能优化研究》为自拟课题。

LSB 隐写术 (LSB Steganography)

- 最早接触隐写术的概念在《密码学》课堂上
- 因为感兴趣曾经使用 Wolfram Mathematica 实现了基本的隐写程序，并写入了博客

支持向量机 (SVM)

- 机器学习是现在非常流行的研究方向，可以在很多领域实现优化
- 完成过 SVM 相关的实战

题目来源

论文题目《神经网络语言模型的性能优化研究》为自拟课题。

LSB 隐写术 (LSB Steganography)

- 最早接触隐写术的概念在《密码学》课堂上
- 因为感兴趣曾经使用 Wolfram Mathematica 实现了基本的隐写程序，并写入了博客

支持向量机 (SVM)

- 机器学习是现在非常流行的研究方向，可以在很多领域实现优化
- 完成过 SVM 相关的实战

所以在毕设中尝试完成应用 SVM 针对 LSB 图像隐写进行优化。

语言模型

隐写是指把一个文件、消息、图像或者视频隐藏到另一个文件、消息、图像或者视频的行为。与密码学不同的是，隐写术旨在隐藏消息或其他形式的信息本身的存在，不引起发送方和接收方以外的人的怀疑而完成信息的交流，而密码学则用于隐藏这些信息的内容，使得非发送方或接收方即使截获消息也无法得到所交流的信息的真实内容。必须满足条件：



语言模型

隐写是指把一个文件、消息、图像或者视频隐藏到另一个文件、消息、图像或者视频的行为。与密码学不同的是，隐写术旨在隐藏消息或其他形式的信息本身的存在，不引起发送方和接收方以外的人的怀疑而完成信息的交流，而密码学则用于隐藏这些信息的内容，使得非发送方或接收方即使截获消息也无法得到所交流的信息的真实内容。必须满足条件：

- 保密性
- 可获得性
- 完整性

隐写分析

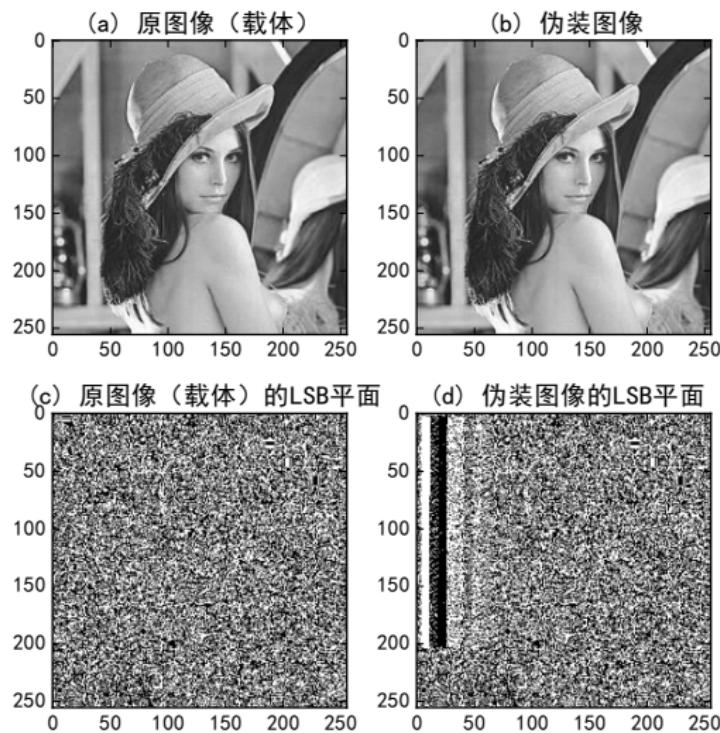
隐写分析

- 视觉隐写分析
- 结构隐写分析
- 统计隐写分析
- 学习隐写分析

隐写分析

隐写分析

- 视觉隐写分析
- 结构隐写分析
- 统计隐写分析
- 学习隐写分析





循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

- 特征向量 \mathbf{x}_i 为图像块的特征



循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

- 特征向量 \mathbf{x}_i 为图像块的特征
- 标签 $y_i \in \{-1, 1\}$ 为安全评估结果，在训练集中由隐写方法评估得到，在使用隐写系统时预测结果作为选择位置的参考指标



循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

- 特征向量 \mathbf{x}_i 为图像块的特征
- 标签 $y_i \in \{-1, 1\}$ 为安全评估结果，在训练集中由隐写方法评估得到，在使用隐写系统时预测结果作为选择位置的参考指标

SVM 分类器

追求最大“间隔”的分类

$$\max_{\mathbf{w}, b} \frac{2}{\|\mathbf{w}\|}$$

$$s.t. \quad y_i (\mathbf{w}^T \mathbf{x}_i + b) \geq 1, i = 1, 2, \dots, N$$



循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

- 特征向量 \mathbf{x}_i 为图像块的特征
- 标签 $y_i \in \{-1, 1\}$ 为安全评估结果，在训练集中由隐写方法评估得到，在使用隐写系统时预测结果作为选择位置的参考指标

SVM 分类器

追求最大“间隔”的分类

过度拟合 & 线性不可分

$$\max_{\mathbf{w}, b} \frac{2}{\|\mathbf{w}\|}$$

$$s.t. \quad y_i (\mathbf{w}^T \mathbf{x}_i + b) \geq 1, i = 1, 2, \dots, N$$



循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

- 特征向量 \mathbf{x}_i 为图像块的特征
- 标签 $y_i \in \{-1, 1\}$ 为安全评估结果，在训练集中由隐写方法评估得到，在使用隐写系统时预测结果作为选择位置的参考指标

SVM 分类器

追求最大“间隔”的分类

过度拟合 & 线性不可分

$$\max_{\mathbf{w}, b} \frac{2}{\|\mathbf{w}\|}$$

■ 核函数：变换特征空间至高维

$$s.t. \quad y_i (\mathbf{w}^T \mathbf{x}_i + b) \geq 1, i = 1, 2, \dots, N$$



循环神经网络

样本集

容量为 N 的训练样本集 $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_N, y_N)\}$

- 特征向量 \mathbf{x}_i 为图像块的特征
- 标签 $y_i \in \{-1, 1\}$ 为安全评估结果，在训练集中由隐写方法评估得到，在使用隐写系统时预测结果作为选择位置的参考指标

SVM 分类器

追求最大“间隔”的分类

$$\max_{\mathbf{w}, b} \frac{2}{\|\mathbf{w}\|}$$

$$s.t. \quad y_i (\mathbf{w}^T \mathbf{x}_i + b) \geq 1, i = 1, 2, \dots, N$$

过度拟合 & 线性不可分

- 核函数：变换特征空间至高维
- 软间隔：以权重 C 容忍分类错误



实验平台和设置

Linux 操作系统

R 主要用于数据统计和图表处理

Python2.7 使用的开发语言和开发环境

Theano 主要的建模语言

实验平台和设置

Linux 操作系统

R 主要用于数据统计和图表处理

Python2.7 使用的开发语言和开发环境

Theano 主要的建模语言

- 同时还依赖于其他的处理脚本，需要对 bash script 和 C/C++ 有足够的了解和掌握；
- GPU 的设备是使用 Titan X，并且对应的 CUDA 版本为 8.0(需要 CUDNN/CUSPARSE 等库的支持)。

SVM 的训练

使用 80 组不同参数进行训练，得到的 SVM 在错误率方面的表现

时间安排

- 2016 年 12 月 ~ 2017 年 1 月 : 整理资料 , 学习研究语言模型的领域知识 ;
- 2017 年 2 月 ~ 2017 年 4 月 : 研究学习深度学习模型的知识 , 特别是循环神经网络的建模过程 ;
- 2017 年 5 月 ~2017 年 7 月 : 调研并实现解决大词表问题的主要手段 , 并实现基本代码框架 ;
- 2015 年 8 月 ~2015 年 10 月 : 实验验证与完善 ;
- 2015 年 11 月 ~2015 年 12 月 : 资料整理和论文撰写 .

Thanks

谢谢各位老师和同学！请大家批评指正；
论文中用到的全部源代码（包括本幻灯片），数据，图像，文档见：
👉 https://github.com/jiangnanHugo/Graduate_Design