# 恶意软件分类方法

汇报人：张鹏

# 目录



01

# 引言

# 恶意软件威胁与增长


## 威胁日益严重

恶意软件数量激增，对网络安全构成严重威胁

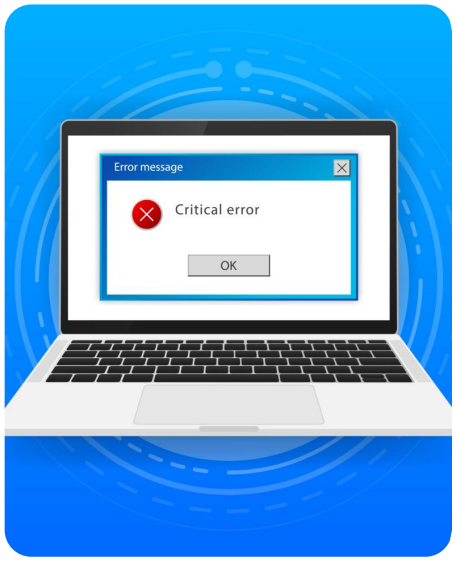

## 增长趋势明显

随着技术发展，恶意软件增长趋势愈发明显

02

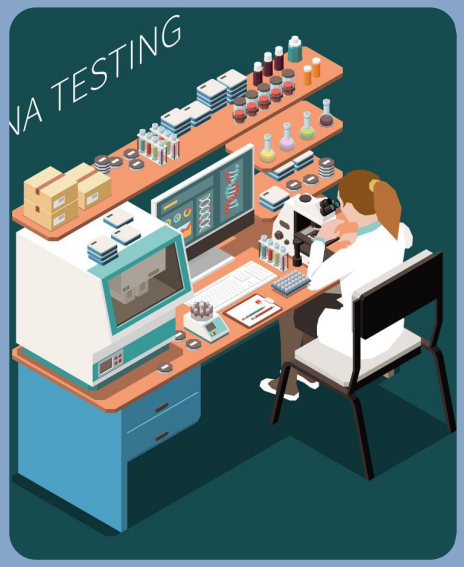
# 恶意软件灰度图像分割

# 基于节类别的分割方法




## 灰度阈值分割

利用灰度阈值进行图像分割




## 边缘检测分割

通过边缘检测算法进行分割


Malware Website

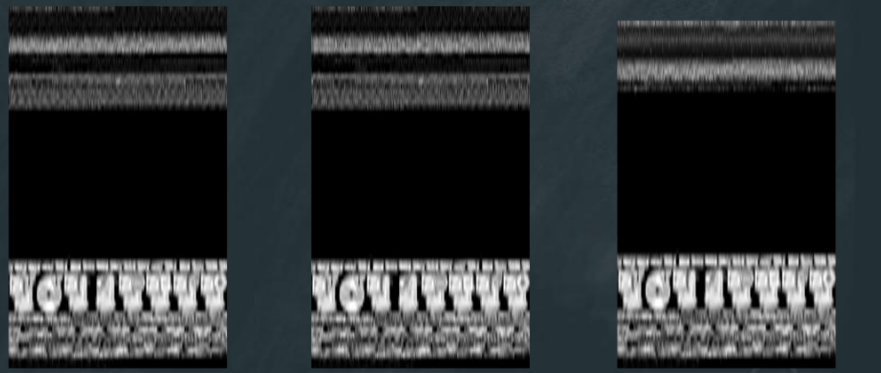
## 区域生长分割

基于像素相似性的区域生长分割

同一家族恶意软件的灰度图像比较。这些恶意软件样本来自微软恶意软件数据集，它只显示了两个恶意软件家族的样本进行比较。

B6nhL5vI2TxV8ODNbRJE D2QZoxVAlsBUkSq6XgHP Gjl3p5gNZxYU7uQH9hSf

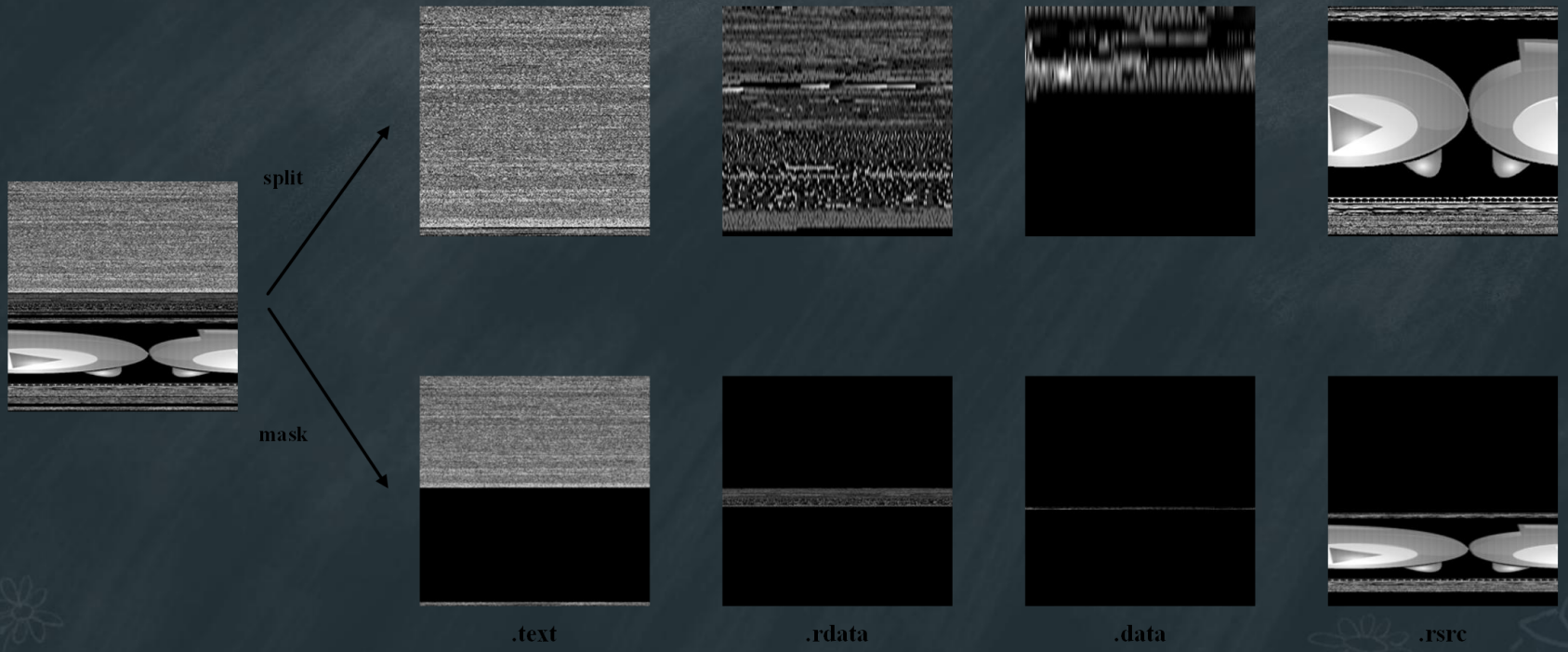
Kelihos_ver3



6ZviYOFyQP8sReVI2HrG bWMTEq0N6d7KRZhvigGQ KGTOj6HAvNqWUcP27bCf

Obfuscator.ACY

# 恶意软件灰度图像的两种分割方法



# 数据集选择与处理

**数据集来源**

选择权威机构发布的数据集

**数据预处理**

清洗、标注、归一化等处理

03

# 实验与评估

# 实验结果

| Model | Dataset(,tag) | Accuracy (training set) | Logloss (test set) |
|---|---|---|---|
| VGG16 | S1 | 99.98% | 0.0401 |
| | S2 | 99.94% | 0.0547 |
| | S3 | 99.94% | 0.0411 |
| | S4(.text+.rdata+.rsrc) | 99.95% | 0.0577 |
| | S5(.text+.rdata+.rsrc) | 99.84% | 0.0889 |
| | S5(imgs-1024+.text+.rsrc) | 99.99% | 0.0521 |
| ResNet50 | S1 | 100% | 0.0316 |
| | S2 | 100% | 0.0330 |
| | S3 | 100% | **0.0265** |
| | S4(.text+.data+.rsrc) | 99.99% | 0.0383 |
| | S4(.text+.rdata+.rsrc) | 99.97% | 0.0320 |
| | S4(.text+.rdata+.data) | 99.93% | 0.0452 |
| | S4(.rdata+.data+.rsrc),T1 | 99.30% | 0.0587 |
| | S4(.text+.rdata+.data+.rsrc) | 99.91% | 0.0364 |
| | S5(.text+.rdata+.rsrc) | 99.95% | 0.0446 |
| | S5(.text+.rdata+.data+.rsrc) | 99.93% | 0.0505 |
| | S5(imgs-1024+.text+.rsrc),T2 | 99.98% | 0.0279 |
| | S5(imgs-1024+.text+.rdata) | 100% | 0.0292 |
| | S5(imgs-1024+.text+.data) | 99.98% | 0.0286 |
| | S5(imgs-1024+.text+.rdata+.data+.rsrc) | 99.97% | 0.0385 |

# 评估指标与讨论

01

### 准确率与误报率

评估分类器性能，分析误报原因

02

### 时间复杂度

分析分类器运行时间，优化算法效率

03

### 讨论与总结

总结实验成果，提出改进方向

06

# 结论与展望

# 方法效果与鲁棒性

## 分类效果优异

方法准确率高，误报率低

## 鲁棒性良好

对未知恶意软件也有较好识别能力

# 研究局限与改进方向

## 数据样本不足

需扩大恶意软件样本库，提高分类准确性

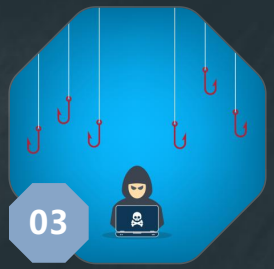


## 分类方法局限

需探索更多分类方法，提高分类效率和精度

## 实时检测挑战

需加强实时检测能力，应对不断变化的恶意软件威胁



# 未来研究方向与前景

## 研究趋势

深入探索恶意软件行为特征

## 前景展望

提升恶意软件检测与防御能力

# 谢谢