

基于 SVM 的 LSB 信息隐藏算法研究与优化

The Study and Improvement of SVM-based LSB Steganography

李欣宜

大连理工大学

📅 2016 年 6 月 13 日

概览

- 1 选题背景
 - 研究背景
- 2 LSB 隐写实现和缺陷分析
 - LSB 隐写研究
 - 隐写分析
- 3 基于 SVM 的优化
 - 隐写方法设计
 - SVM 的训练和预测
- 4 实验与结果
 - 实验环境
 - 实验结果

题目来源

论文题目《基于 SVM 的 LSB 信息隐藏算法研究与优化》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 (<https://www.yangzhou301.com/2015/11/15/861014670/>)

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
(https://github.com/Lixinyi-DUT/machine_learning_techniques)

所以在毕设中尝试完成应用 SVM 针对 LSB 图像隐写进行优化。

隐写术

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

LSB 图像隐写

秘密消息 需要隐藏的信息

载体 cover 用来隐藏信息的文件，多媒体文件因为包含的数据巨大，适合作为载体。在本文中选取像素图像为载体。

伪装 stego 隐藏了秘密消息的文件，与载体图像看上去没有区别

最低有效位 LSB 数据的最低位，对于 8 位二进制为第 0 位

像素值	7	6	5	4	3	2	1	0
1	1	1	0	0	0	1		
1	0	0	0	1	0	0		
0	1	1	1	1	1	1	0	
1	1	1	0	0	0	1		
1	0	0	0	1	0	0		
0	1	1	1	1	1	1	0	
1	1	0	1	1	1	1		
1	0	0	0	1	0	0	0	

LSB 图像隐写

秘密消息 需要隐藏的信息

载体 cover 用来隐藏信息的文件，多媒体文件因为包含的数据巨大，适合作为载体。在本文中选取像素图像为载体。

伪装 stego 隐藏了秘密消息的文件，与载体图像看上去没有区别

最低有效位 LSB 数据的最低位，对于 8 位二进制为第 0 位

像素值	7	6	5	4	3	2	1	0
226	1	1	1	0	0	0	1	0
136	1	0	0	0	1	0	0	0
124	0	1	1	1	1	1	0	0
226	1	1	1	0	0	0	1	0
137	1	0	0	0	1	0	0	1
124	0	1	1	1	1	1	0	0
223	1	1	0	1	1	1	1	1
137	1	0	0	0	1	0	0	1

LSB 图像隐写

秘密消息 需要隐藏的信息

载体 cover 用来隐藏信息的文件，多媒体文件因为包含的数据巨大，适合作为载体。在本文中选取像素图像为载体。

伪装 stego 隐藏了秘密消息的文件，与载体图像看上去没有区别

最低有效位 LSB 数据的最低位，对于 8 位二进制为第 0 位

秘密消息

'a' = 0b01100001

像素值	7	6	5	4	3	2	1	0
226	1	1	1	0	0	0	1	0
136	1	0	0	0	1	0	0	0
124	0	1	1	1	1	1	0	0
226	1	1	1	0	0	0	1	0
137	1	0	0	0	1	0	0	1
124	0	1	1	1	1	1	0	0
223	1	1	0	1	1	1	1	1
137	1	0	0	0	1	0	0	1

LSB 图像隐写

秘密消息 需要隐藏的信息

载体 cover 用来隐藏信息的文件，多媒体文件因为包含的数据巨大，适合作为载体。在本文中选取像素图像为载体。

伪装 stego 隐藏了秘密消息的文件，与载体图像看上去没有区别

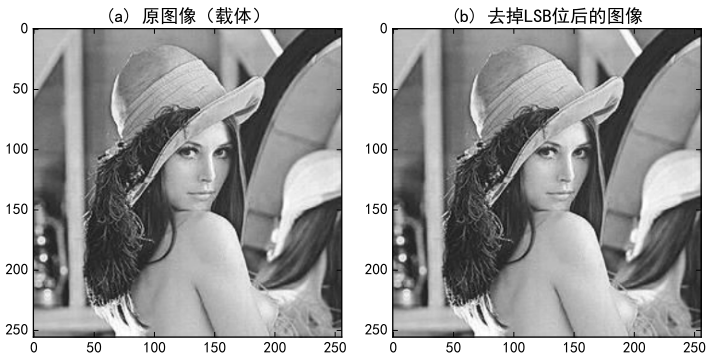
最低有效位 LSB 数据的最低位，对于 8 位二进制为第 0 位

秘密消息

'a' = 0b01100001

像素值	7	6	5	4	3	2	1	0
226	1	1	1	0	0	0	1	0
137	1	0	0	0	1	0	0	1
125	0	1	1	1	1	1	0	1
226	1	1	1	0	0	0	1	0
136	1	0	0	0	1	0	0	0
124	0	1	1	1	1	1	0	0
222	1	1	0	1	1	1	1	0
137	1	0	0	0	1	0	0	1

LSB 图像隐写的实现



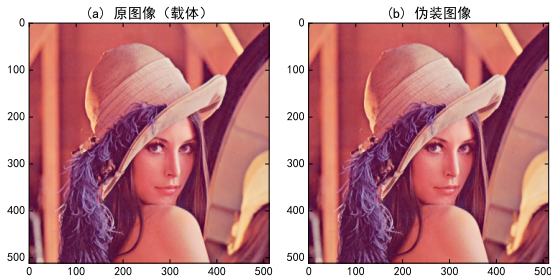
8bit 灰度图像截去 LSB 平面前后无明显变化

图像的 LSB 平面的变化不会带来强烈的视觉变化

LSB 图像隐写的实现

顺序嵌入

先将秘密消息的长度 l 转化为二进制数嵌入在图像的前 n 位，再按照图像的自然顺序将秘密消息逐个嵌入接下来的像素

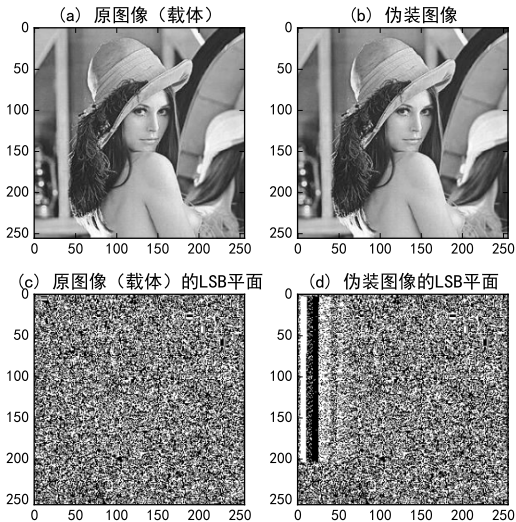


消息提取

先提取前 n 个像素的 LSB 位获得消息长度 l ，再读取接下来的 $8l$ 个像素的 LSB 位恢复完整的消息

隐写分析

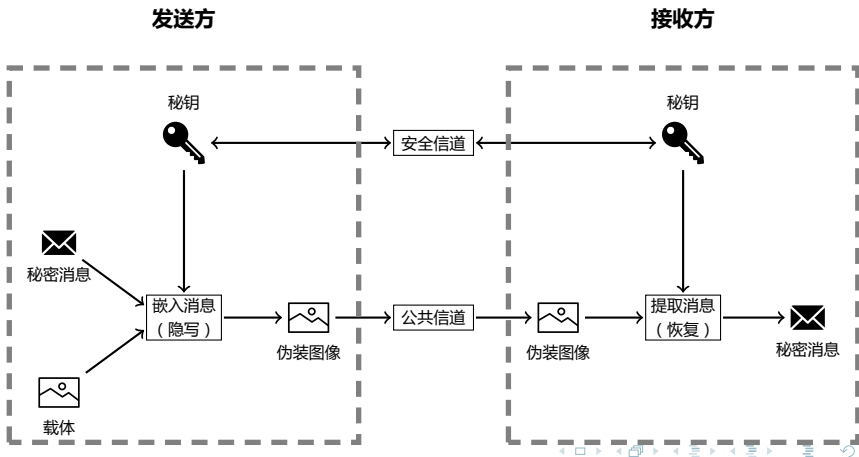
- 视觉隐写分析
- 结构隐写分析
- 统计隐写分析
- 学习隐写分析



密钥隐写系统

引入密钥的隐写系统

将密钥作为 PRNG 的种子，确定隐藏的像素序列



针对 LSB 的图像隐写分析

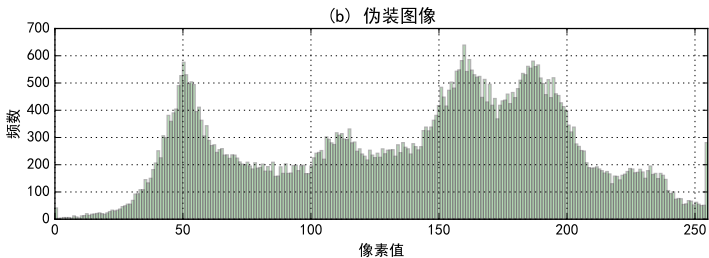
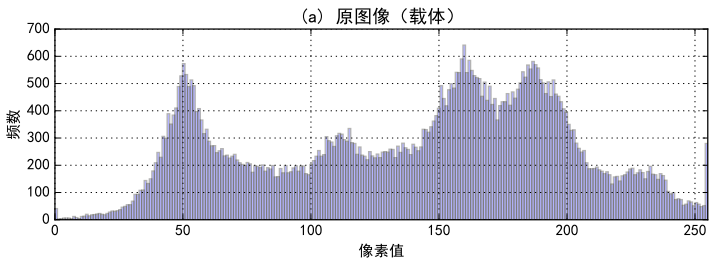
- 密钥隐写系统对双方的通信资源要求较高
- 存在可以攻破随机位置隐写的 LSB 图像分析方法

经典的 LSB 图像分析方法

本文中实现了这些方法用于评估伪装图像的安全性

- χ^2 检测
- 样本对分析 (SPA)
- RS 隐写分析

χ^2 检测



χ^2 检测

原理

由于 LSB 修改的过程实际可用看做像素值 $2i$ 与 $2i+1$ 间的变换，相比自然图像，秘密消息的嵌入使得值对 $(2i, 2i+1)$ 间的分布更接近均匀分布。

实现方法

计算

$$S_{PoV} = \sum_{i=0}^{127} \frac{\left[h_{2i} - \frac{1}{2} (h_{2i} + h_{2i+1}) \right]^2}{\frac{1}{2} (h_{2i} + h_{2i+1})}$$

查询 χ^2 分布表我们可以计算对应的 p 值，用以度量图像为伪装图像的概率，根据 p 值大小决定该图像是否包含隐藏消息。

样本对分析

原理

在 LSB 嵌入后，我们可以获得一个描述变多重集合间转换的有限状态机。统计样本对频率可以分析得到消息长度。

实现方法

解方程估算秘密消息的长度

$$\frac{p^2}{4} (2|C_0| - |C_{j+1}|) - \frac{p}{2} \left[2|D'_0| - |D'_{2j+2}| + 2 \sum_{m=0}^j (|Y'_{2m+1}| - |X'_{2m+1}|) \right] + \sum_{m=0}^j (|Y'_{2m+1}| - |X'_{2m+1}|) = 0$$

对于仅使用最低位隐藏消息的 LSB 隐写，代入 $i = 126$ 解出消息长度 p ，若为负或者小于一个固定值可以判断为不存在隐藏消息。

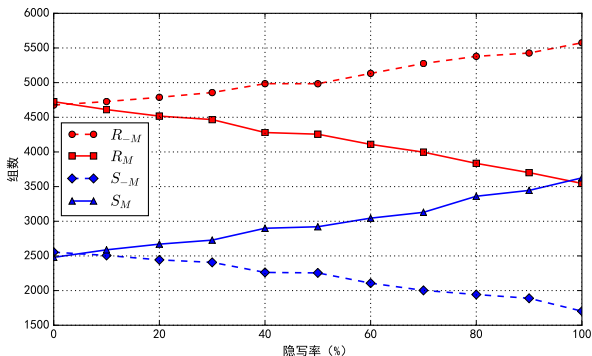
RS 隐写分析

原理

正翻转 F_1 是像素值在 $2i$ 和 $2i+1$ 间的转换

负翻转 F_1 是像素值在 $2i-1$ 和 $2i$ 间的转换

将图像分为小块(组), 自然图像和伪装图像在进行正负翻转后平滑度的变化趋势不同



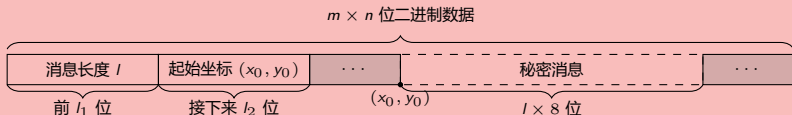
可行性与优化目标

应用场景假设

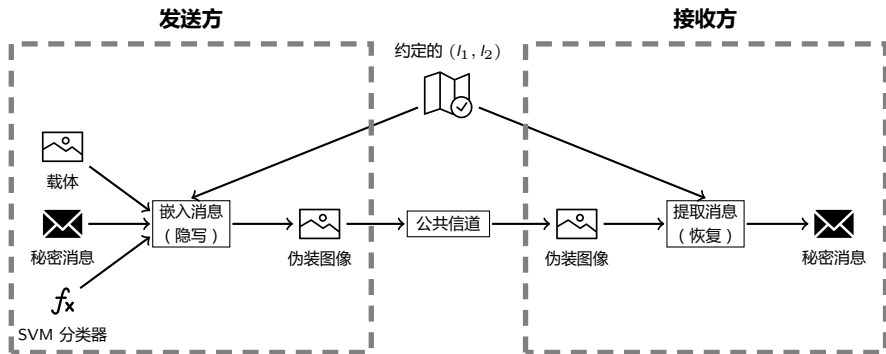
- 无法获得安全信道交换密钥
- 但可以预先约定少量信息

思考

- 选择合适的位置（图像块）可以在一定程度上抵抗隐写分析
- 根据一些特征判断某个位置是否能安全隐藏消息，实际上是一个 SVM 分类问题
- 隐藏消息的图像块信息也可以作为一个辅助信息隐藏在前几位像素，为了使辅助信息尽量少，选择边长为 $\lceil 2\sqrt{2}l \rceil$ 像素的正方形



引入 SVM 的隐写系统



支持向量机 (SVM)

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

$$\begin{aligned} \max_{\mathbf{w}, b} \quad & \frac{2}{\|\mathbf{w}\|} \\ \text{s.t.} \quad & y_i (\mathbf{w}^T \mathbf{x}_i + b) \geq 1, i = 1, 2, \dots, N \end{aligned}$$

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

特征选择

方差

表示图像块像素值的离散程度

$$\text{var}(B) = \frac{\sum_{i=1}^m \sum_{j=1}^n (x_{i,j} - \bar{x})}{m \cdot n - 1}$$

整体差异度

图像块与整个载体在像素值分布方面的差异

$$D_{B,I} = \sum_{i=0}^{255} [\text{fre}(B)_i - \text{fre}(I)_i]^2$$

图像块是否“突出”

特征选择

sc 匹配度

图像块的 LSB 平面与秘密消息的 LSB 平面的匹配程度

$$sc_match = \frac{\sum_{i=1}^{8l} p(M_{Binary}(i) = B_{LSB}(i))}{8l}$$

平滑度

沿用 RS 隐写分析中的平滑度定义并加以扩充完善，表示邻接像素之间的差异程度，邻接像素为所有方向上的邻接像素

$$S_i = \{x_{i\leftarrow}, x_{i\rightarrow}, x_{i\uparrow}, x_{i\downarrow}\}$$

提出使用矩阵偏移的方法避免重复并提高了计算效率

$$AD_{\rightarrow} = |B((1, 1), (m, n - 1)) - B((1, 2), (m, n))|$$

实验平台和设置

Windows10 操作系统

MATLAB2015b 主要的图像处理、数据计算平台和语言

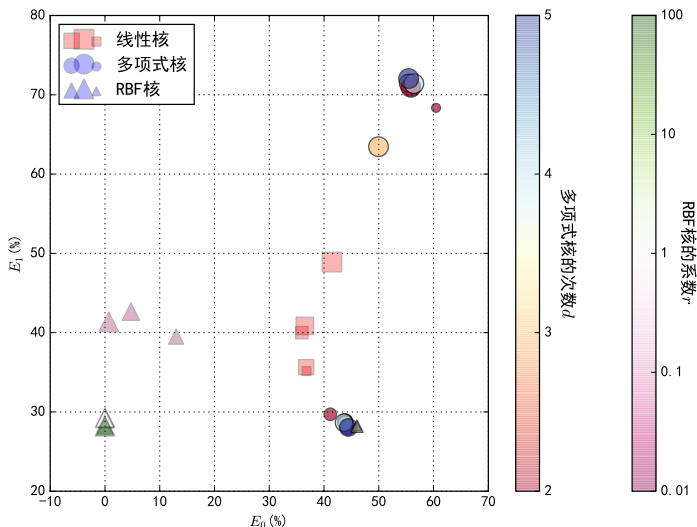
Python3.5 完成了一些数据预处理、收集和绘制图像的任务

UCID 图像数据集，包含 1338 张彩色图像，为方便处理在实验中全部转换为灰度图像

- 训练阶段使用嵌入率为 5%-50% 的 2000 个图像块（在图像数据集中随机抽样）样本训练不同参数的 SVM，并使用 200 个图像样本作为检验集进行调整
- 预测阶段使用嵌入率分别为 5%-50%（步长 5%）的 13380 样本（1338 张图像，每张 10 个位置）验证 SVM 的分类准确率，隐写系统在安全方面的提升依赖于 SVM 的预测准确率。

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

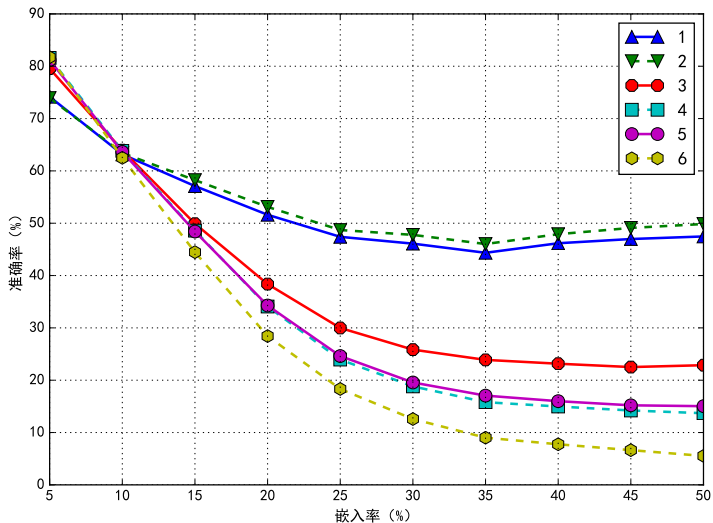


挑选 6 组性质典型的 SVM

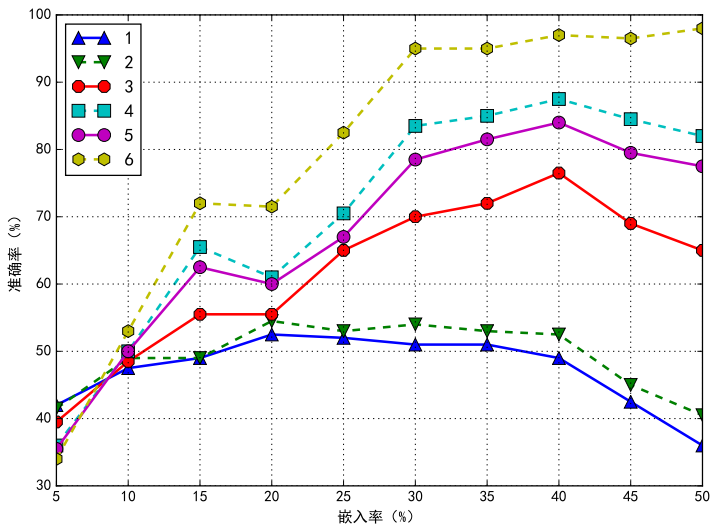
TABLE – 6 组 SVM 的参数

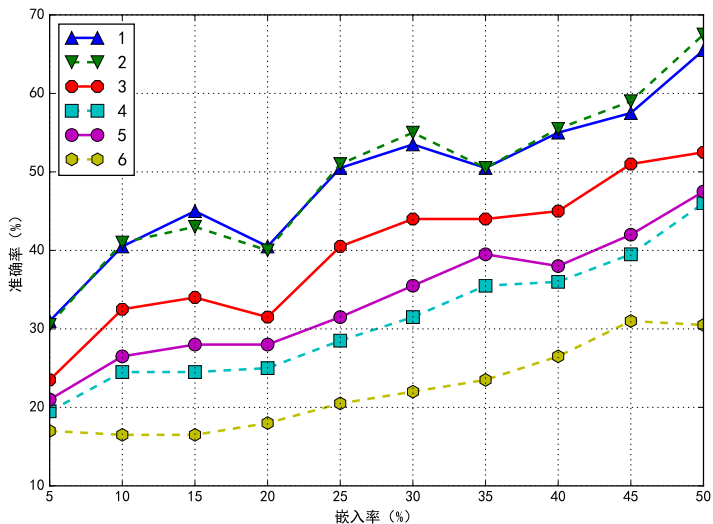
编号	核类型	代价 C	次数 d	系数 γ	训练错误率 E_0	检验错误率 E_1	支持向量数
1	线性核	0.01	1	1	36.8	35.15	1566
2		1		1	36.75	35.65	1045
3		0.1	2	1	41.15	29.7	208
4	多项式核	0.1	4	1	43.8	28.65	90
5		10	4	0.1	43.65	28.65	83
6	RBF 核	1	无穷大	1	0.2	28.95	2000

对抗 RS 隐写分析



对抗 SPA



χ^2 测验

Thanks

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/Lixinyi-DUT/graduation-project>