

基于 Haar 小波域指标自适应选择载体的 JPEG 隐写*

黄 炜¹, 赵险峰²



¹(厦门大学 软件学院, 福建 厦门 361005)

²(信息安全国家重点实验室(中国科学院 信息工程研究所), 北京 100093)

通讯作者: 黄炜, E-mail: whuang@xmu.edu.cn

摘 要: 为了解决目前图像纹理复杂度建模的隐写载体选择指标难以有效适用于 JPEG 隐写的问题, 提出一种基于 Haar 小波域指标自适应选择载体的 JPEG 隐写方法, 以高阶 Haar 小波变换模型建立 JPEG 图像像素关系, 计算各方向上的分解图像矩阵的范数均值, 用于选择难以被检测的载体. 该指标比已有方法的像素间建模能力更强, 更能反映 JPEG 隐写所影响的像素间关系, 且能增强 JPEG 隐写的隐蔽性. 实验结果表明, 在大多数情况下, 与现有载体选择指标相比, 该方法与隐写隐蔽性具有更高的相关性. 使用该方法优选的载体进行隐写, 比优选前的隐蔽性提高约 7.7%, 比用现有指标优选载体的 JPEG 隐写方法的隐蔽性平均提高约 2.0%. 因此, 该方法隐写具有更高的隐蔽性.

关键词: 隐写; 载体选择; Haar 小波; 范数

中图法分类号: TP309

中文引用格式: 黄炜, 赵险峰. 基于 Haar 小波域指标自适应选择载体的 JPEG 隐写. 软件学报, 2018, 29(8): 2501-2510. <http://www.jos.org.cn/1000-9825/5281.htm>

英文引用格式: Huang W, Zhao XF. JPEG steganography based on adaptive cover selection using Haar wavelet domain indicators. Ruan Jian Xue Bao/Journal of Software, 2018, 29(8): 2501-2510 (in Chinese). <http://www.jos.org.cn/1000-9825/5281.htm>

JPEG Steganography Based on Adaptive Cover Selection Using Haar Wavelet Domain Indicators

HUANG Wei¹, ZHAO Xian-Feng²

¹(Software School, Xiamen University, Xiamen 361005, China)

²(State Key Laboratory for Information Security (Institute of Information Engineering, The Chinese Academy of Sciences), Beijing 100093, China)

Abstract: The existing steganographic cover selection indicators based on image texture complexity modeling are not compatible with JPEG steganography. To solve this problem, a JPEG steganography is proposed based on cover selection using Haar wavelet domain indicators. This method establishes the relationship of JPEG image pixels by taking high-ordered Haar wavelet translation as the model, and calculates the average norm of the decomposition image matrix in each direction to select highly undetectable covers. Moreover, the proposed indicator, which performs better than most of the existing models in the inter pixel modeling ability, can enhance the concealment of JPEG steganography in cover selection. Experimental results show that, in most cases, the proposed JPEG steganography using cover selection achieves higher concealment than that without selecting covers by an average value of about 7.7%. This figure has

* 基金项目: 福建省自然科学基金计划青年创新项目(2018J05112); 国家自然科学基金(61402390, U1636102); 国家科技支撑计划(2014BAH41B01); 国家重点研发计划(2016YFB0801003)

Foundation item: Fujian Natural Science Foundation Program Youth Innovation Project (2018J05112); National Natural Science Foundation of China (61402390, U1636102); National Key Technology R&D Program of China (2014BAH41B01); National Key Research and Development Program of China (2016YFB0801003)

收稿时间: 2016-09-14; 修改时间: 2016-12-10; 采用时间: 2017-03-15; jos 在线出版时间: 2017-07-12

CNKI 网络优先出版: 2017-07-12 15:33:21, <http://kns.cnki.net/kcms/detail/11.2560.TP.20170712.1533.003.html>

higher concealment than the existing cover selection indicators by an average value of 2.0%. Therefore, the proposed steganography attains better concealment.

Key words: steganography; cover selection; Haar wavelet; norm

隐写术(steganography)^[1]是一种信息隐藏技术,它通过编码将隐蔽信息藏于主流媒体中来掩盖通信的事实.随着 JPEG 图像的广泛使用,以 JPEG 为载体的隐写成为研究人员关注的重点之一.相应地,隐写分析(steganalysis)^[2]则是检测给定信号中隐写行为存在性或存在可能性的技术,它通常借助统计或模式分类的方法预测给定信号存在隐写行为的可能性.现有文献中,衡量隐写算法在通用配置下的优劣指标主要为隐蔽性,一般是指该隐写算法所嵌入的一组图像在隐写分析时的平均错误率^[3].如果错误率较高、较难被准确检测,则认为隐写算法是较安全的^[4].因而,提高隐写算法的隐蔽性,对保护个人的隐私和企业的商业秘密具有现实意义.

高隐蔽性隐写方法主要通过 3 个方面增强隐蔽性:(1) 通过密钥置乱图像像素,将隐蔽信息随机分散到图像的不同位置^[5];(2) 结合编码学方法减少扰动像素或 JPEG 系数数量^[6]等;(3) 利用校验网格码(syndrome trellis code,简称 STC)^[7]等编码方法,自适应选择在总体代价之和较小的位置嵌入.目前,空域最有效的空域通用小波隐写(S-UNIWARD)^[8]和最小化最优检测器的功率(MiPOD)^[9]等算法以及 JPEG 隐写最有效的边信息通用小波隐写(SI-UNIWARD)^[8]、JPEG 通用小波隐写(J-UNIWARD)^[8]等都采用该方法,极大地提高了隐写隐蔽性.自适应隐写方法通常将图像的纹理属性作为代价函数,故可知,图像中纹理复杂程度与隐写分析准确率有一定的联系.

现有的通用隐写分析方法通常提取图像特征并选用合适的分类器进行训练和预测,其中,对 JPEG 图像隐写最有效的特征之一是 22 510 维校准富模型特征(CC-JRM)^[10],而最有效的低维特征之一是联合校准特征^[11].上述两种特征主要通过对待测图像截取 4 行 4 列重新压缩以估计原图像,计算图像的灰度共生矩阵来刻画图像像素间的关系,具有很好的效果.这说明,用于刻画图像像素间关系的指标与隐写分析准确率有一定的相关性.

学者们^[4,12-15]已意识到,隐写行为的隐蔽性不仅与隐写算法设计有关,也受载体图像的选择的影响.载体选择是指在多样本隐写的环境^[16]下选出一类隐写准确率较低的图像用于嵌入,可以进一步提升隐蔽性.载体选择方法可按隐写者对隐写分析者的掌握程度分为无知识、部分知识和全知识这 3 类^[13].其中,无知识的方法通常对某个影响隐写隐蔽性的图像属性计算评价指标,作为载体选择的依据,计算复杂度低,适合于在便携设备等情形下使用.除了较为直观的图像尺寸、可嵌入位置和 JPEG 质量因子之外^[13],还有纹理复杂度评价指标.全知识类^[17,18]需要隐写分类器的反馈,其中,构造隐写分类器、提取特征等环节计算量很大.部分知识类^[19]则需要反复生成隐写图像用以计算载体和隐写图像之间的相似度,运行耗时长.

目前用于载体选择的图像纹理复杂度指标,在指示空域位图隐写隐蔽性方面取得了很好的效果,却不能很好地指示 JPEG 隐写隐蔽性.主要指标包括信息熵^[14]、局部方差^[12]和线性预测误差法^[15]等.信息熵方法仅与图像的直方图特性有关,对纹理的指示作用较弱;局部方差以水平或垂直位置相邻两个像素间差值平方和为指标,仅考虑相邻像素间的线性关系;线性预测误差法则用最近的 8 或 24 个像素预测中央的像素,将预测均方误差作为指标,仅考虑了 3×3 或 5×5 分块像素间的线性关系.事实上, JPEG 编码的有损压缩是非线性的,对 JPEG 量化系数的改变反映为空域上 8×8 像素分块的变化,因而上述线性的载体选择指标具有提高的空间.

为了解决目前图像纹理复杂度隐写载体选择指标难以有效适用于 JPEG 隐写的问题,本文提出一种基于 Haar 小波指标自适应选择载体的 JPEG 隐写.该方法对图像做高阶 Haar 小波变换,计算各方向上的分解图像矩阵的范数作为载体选择的指标.该指标采用的小波域模型比已有方法的模型像素间建模能力更好.在公开图像和隐写算法下的实验下,本文方法与隐写分析准确率的 Spearman 秩相关系数^[12]比现有主要载体选择指标平均高约 0.027,优选后隐写隐蔽性在原基础上提高约 7.7%,比现有载体选择指标平均高约 2.0%.实验结果表明,使用其优选的载体进行隐写,在原有隐写算法基础上提高了隐蔽性,在大多数情况下比现有图像纹理指标效果要好.

本文第 1 节描述载体选择问题的模型.第 2 节列举现有的载体选择指标,包括信息熵法、局部方差法、线性预测误差法等,并说明其对 JPEG 隐写和隐写分析的局限性.第 3 节介绍本文方法,即 Haar 小波分解图像及高阶统计量,从理论上探讨其与 JPEG 隐写特征之间的关系.第 4 节介绍实现流程.第 5 节通过实验比较随机选择、已有方法和本文方法载体选择在不同条件下隐写分析的准确率.最后总结全文.

1 载体选择问题模型

本文探讨隐写者对隐写分析者无知识的载体选择问题,模型如下.

假设隐写者制备得到一组图像 $c=\{c_1, c_2, \dots, c_n\}$, 选择其中部分的图像, 将长度为 m 的隐蔽信息分片并依次嵌入. 最终得到需要发送的图像为 $x=\{x_1, x_2, \dots, x_n\}$, 其中, $x_i=c_i$ 或 $x_i=E(c_i, m_i, k)$, E 为隐写算法, m_i 为信息分片, k 为密钥. 设存在某种评价指标 $f(x)$ 对任何图像 x 计算出一个数值, 可以在某个给定一组阈值 $\{F_j\}$ 之下估算所有符合 $f(x) \in (F_{j-1}, F_j]$ 的一组图像在隐写分析时的平均错误率 ε_j . 由于隐写者对隐写分析者无知识的情况下很难估计 ε_j , 一般地, $f(x)$ 和 ε_j 存在一定的 Spearman 秩相关性.

由于隐写算法对图像的修改量较为轻微, 图像 x 的评价指标 $f(x)$ 在隐写前后变化不大, 且对于隐写者和隐写分析者是公开的. 隐写分析者有能力根据接收到的图像预测其可能的准确程度调整在综合决策时的参考权重. 隐写者也可以根据 $f(x)$ 选择适合隐写的一组载体图像序号 I , 所有 $i \in I$, 选择不隐写, 即 $x_i=c_i$; 而对任何 $i \in I$, 选择隐写嵌入信息, 即 $x_i=E(c_i, m_i, k)$. 为了防止被隐写分析者检测出, 隐写者应使得在该种选择下, 在 $i \in I$ 时, 隐写分析者的错误率尽量大, 即隐写者应使隐写分析者在检测载体图时能够较准确且较有把握地将其判为不含隐写, 而检测隐写图像时尽量做出准确率较低的判定.

2 已有基于图像纹理的载体选择指标和方法

在现有文献中提出的载体选择指标和方法中, 可指示隐蔽性用于载体选择的指标主要有 3 种.

- (1) 信息熵(entropy). 信息熵法计算图像像素灰度值的熵值 $f_{ENT} = \sum (-p_i \log p_i)$ 作为图像复杂度指标, 其中, p_i 表示图像中灰度值 i 出现的概率. 图像的熵越大, 图像灰度值越丰富, 隐写的隐蔽性越强.
- (2) 局部方差(local variance, 简称 LV). 局部方差法先计算相邻两个像素之间的差值, 再对差值求方差, 以横向和纵向的方差均值为指标, 即以 $f_{LV} = \frac{1}{2} \sum [(x_{i,j} - x_{i-1,j})^2 + (x_{i,j} - x_{i,j-1})^2]$ 为指标, 其中, $x_{i,j}$ 是位置 (i,j) 上的像素灰度值. 一般局部方差越大的图像, 相邻像素之间变化剧烈, 纹理越丰富, 隐写的隐蔽性越强.
- (3) 线性预测误差(linear prediction error, 简称 LPE). 线性预测误差法在局部方差利用相邻像素预测的基础上, 采用了线性预测模型 $\hat{x}_{i,j} = \beta N(x_{i,j}, k) + \varepsilon$, 即以像素 $x_{i,j}$ 的 k 阶邻接像素 $N(x_{i,j}, k)$ 的线性方程来预测 $x_{i,j}$, 将预测误差 $f_{LPE} = \sqrt{\sum (x_{i,j} - \hat{x}_{i,j})^2}$ 作为指标. 预测误差越大, 建模越困难, 隐写隐蔽性越强.

然而, 上述指标不可避免地存在以下不足: 第一, 信息熵方法只与图像像素灰度值的概率分布函数有关, 缺乏像素在图像中位置的信息, 因而难以很好地指示该类图像在隐写分析时的难易程度; 第二, 局部方差法只考虑了相邻两个像素的差值, 即便 k 阶 LPE 方法也仅限于一个像素周围 $(2k+1)^2 - 1$ 个像素的关系. JPEG 隐写受 JPEG 编码 8×8 像素分块的 DCT 变换、量化和反量化等的影响, 不仅应考虑像素与紧邻周围的像素的相关性, 还应该考虑更大范围的像素对隐写行为的影响, 从而设计更复杂的纹理复杂度评价模型, 如小波域模型.

3 小波域的载体选择指标

3.1 小波变换简介

小波变换是一种将信号数据分割成不同频率成分的工具. 从滤波器组的角度, 原始信号经低通、高通滤波和下采样等处理得到低频和高频成分, 分别表示图像的总体和细节信息. 以 SI-UNIWARD 算法所用的 Daubechies 小波(消失矩为 8)为例, 其高通滤波器采用 $g=[-0.0544, 0.3129, -0.6756, 0.5854, 0.0158, -0.2840, -0.0005, 0.1287, 0.0174, -0.0441, -0.0140, 0.0087, 0.0049, -0.0004, -0.0007, -0.0001]$, 低通滤波器则采用 $h=[-0.0001, 0.0007, -0.0004, -0.0049, 0.0087, 0.0140, -0.0441, -0.0174, 0.1287, 0.0005, -0.2840, -0.0158, 0.5854, 0.6756, 0.3129, 0.0544]$. 分别用 $h \cdot g^T, g \cdot h^T, g \cdot g^T$ 对信号做卷积后得到一阶 LH, HL 和 HH 方向的降解, 重复降解与下采样可得到更高阶的降解.

3.2 JPEG隐写在小波域的变化

研究人员认为,一些在纹理复杂的区域嵌入信息较难检测.在PQ的衍生版本^[6]中,PQe 优先嵌入在能量大的区域和 PQt 优先嵌入在纹理复杂的区域,因而隐蔽性有显著提升.在 SI-UNIWARD,J-UNIWARD 等方法中,更是利用修改前后小波系数的差值作为选择嵌入位置的权重.通常,计算能量和纹理采用的是像素间差值或系数平方和的方法,只能计算 8 个相邻方向上的差异.而小波系数的表示范围更广,可以求取不同方向上的像素差值.

通过比较高隐蔽性隐写算法的嵌入位置的共同点,可知嵌入某些位置的隐蔽性高于其他区域.本文选取 MME3^[5]、PQe、PQt 和 nsF5 等隐写算法,它们虽然都不以小波域特征选择嵌入位置,但在纹理复杂区域嵌入比较密集.以 BOSSBase 图像库序号为 52 的图像为例(图 1(a)),其纹理较为复杂的区域是山与天空的交界处和水面的波纹处.通过对原图像与不同隐写算法 0.05bpac(bit per non-zero AC coefficient,简称 bpac)隐写图像求差值,可以得到这些算法的嵌入位置(图 1(b)~图 1(e)).从图中可以看出,其共同特点是山峰与天空交界处及水面波纹处的改动量大于其他位置的改动量.对上述原图像做小波变换求取高频 HH 分量(图 1(f))可知,纹理复杂的区域集中在小波变换的 HH 分量上.小波分解图像中系数大的区域,正是高隐蔽性隐写算法所共同优先选择的位置.

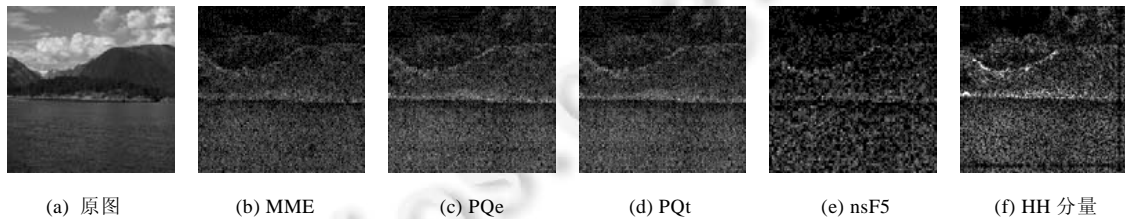


Fig.1 Comparison of the original image, embedded positions of different steganographic images (in 0.05 bpac), and the HH decomposition image of the original one

图 1 原图像、各种隐写算法(0.05 bpac)隐写图像的嵌入位置与原图小波 HH 分量图对照

JPEG 与空域隐写相比增加了 DCT 变换和量化等过程,周围像素差值大的位置无法像空域隐写直接判定为较难隐写分析的位置.但是相邻像素值差异较大的区域,DCT 变换及量化后表现为高频区域系数较大,统计较不稳定,不利于隐写分析.因此,统计图像高频分量变化情况,对选出较难被隐写分析的载体具有现实的可行性.

相应地,从隐写分析角度而言,当前最有效的若干种 JPEG 隐写特征(如 CCJRM 和 DCTR 特征等)主要计算 JPEG 量化系数的共生矩阵.其中,CCJRM 计算 JPEG 量化系数在水平、竖直和对角线等各个方向上的共生矩阵,将块间和块内等系数残差合并成为最终高维特征.DCTR 特征则是将 JPEG 图像解码至空域,并将每一块的像素与 DCT 基础模式矩阵作卷积,再计算卷积得到的矩阵的直方图.该过程也可视为对空间上相邻 4 个分块的 256 个系数做正交投射.JPEG 量化系数的一阶或高阶概率分布模型(如直方图、共生矩阵)在 JPEG 隐写分析上起着重要的作用,能够反映 JPEG 隐写对自然图像的修改.这些特征在处理量化系数时不仅考虑局部的系数间关系,还考虑了相邻分块间的系数关系.相邻分块间的系数关系,是现有基于线性的载体选择指标无法描述的.

小波域系数的特征与隐写分析特征设计上有着较好的一致性.离散小波变换从本质上是一种卷积运算,同时,小波变换是正交的,这一特性可以有效保持图像的多样性,这与 DCTR 特征使用正交投射的目的是相近的.小波变换的多尺度特性还可以刻画不同范围的图像内容信息.现有特征在设计时,也采取了同时考虑分块间和分块内的 JPEG 量化系数关系的做法.因此,从隐写分析角度而言,采用小波域的指标刻画隐写的隐蔽性具有可行性.

3.3 小波域指标

由上一节可知,JPEG 隐写在纹理复杂或能量较高的分块或位置进行嵌入较难被检测到.即便测试的算法并非以小波域指标为代价函数,这类区域在小波域上仍集中反映为高频降解图像中系数较大的区域.本文设计了一种指标,反映图像高频降解图像包含较大系数的数量,从而用于指示图像隐写被检测出的难易程度.

首先,对图像 X 进行离散小波变换.使用高低通滤波器对图像做二维卷积,分别在水平和垂直方向上进行卷积,并对上述结果做步长为 2 的下采样,得到 3 个方向上的第 1 级小波分解图像,包括 $W^{LH}=(g*h^T*X)\downarrow 2$, $W^{HL}=(g^T*h*X)\downarrow 2$

$(h * g^T * X) \downarrow 2$ 和 $W^{HH} = (g * g^T * X) \downarrow 2$. 随后对 W^{HH} 继续分解, 得到第 2 级的小波分解图像. 不断重复上述步骤, 得到更高级的小波分解图像. 一般地, 第 1 级~第 3 级小波分解已可以表示图像的细部纹理特征. 由于 JPEG 隐写通常是在 8×8 分块上进行的, 第 3 级小波在两个方向上都经过了 3 次下采样, 即每个分块被下采样为 1 个系数. 因此, 级数再往上时, 高频部分不再表示细部的纹理特征, 参考意义不大.

由于小波分解图像的维度大, 不宜直接作为选择载体指标, 需要将其降至一维标量. 我们尝试过不同的小波分解方法以及各种指标, 包括一阶、二阶和三阶范数等多种统计量. 其区别在于分解图像中绝对值大的系数对整幅图像指标值的占比, 阶数越高, 含有绝对值大的系数的图像越适合作为载体图像. 本文采用的计算公式为

$$f_{WB} = \frac{1}{3} \left[(\sum |W_{u,v}^{h,k}|^r)^{-r} + (\sum |W_{u,v}^{v,k}|^r)^{-r} + (\sum |W_{u,v}^{d,k}|^r)^{-r} \right] \quad (1)$$

其中, k 是小波变换的阶数, r 是小波分解图像系数范数的阶数. 实验对比发现, 一般三阶 Haar 小波的一阶距表现较好, 即取 $k=3, r=1$. 此时, Haar 小波高通滤波器采用 $g = \left[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right]$, 而低通滤波器采用 $h = \left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right]$. 不同隐写算法和隐写特征对小波分解图像的各个方向修改量并不完全相同, 因此, 为使指标能够稳定地适用于不同的隐写算法和隐写特征, 在设计时, 对水平、竖直和对角线等 3 个方向求取均值, 即它们的权重是相等的.

3.4 与已有载体选择指标的关联

本文提出的载体选择指标与 LV, LPE 指标在原理上有一定的相同点. 这些指标都假设图像像素之间具有相关性, 利用图像中的像素与相邻像素之间的关系来对图像纹理特性建模. 通过评价该载体的纹理特性, 指示该载体用于隐写的隐蔽性.

本文方法在原理上与已有方法也有明显区别. LV 考察的是像素点与横向和纵向相邻像素点之间的关系, LPE 考察的则是像素点与周围 8 个 (LPE1)、24 个 (LPE2) 像素点之间的差异. 与 LV, LPE 反映线性关系不同的是, 本文方法采用小波变换, 考虑了图像像素的非线性关系. 虽然一阶 Haar 小波变换是像素间的差值关系, 但是本文方法涉及 2 阶及以上 Haar 小波变换, 可以展示不同缩放尺寸下的像素间关系. 图像熵的原理则与 LV、LPE、本文方法区别较大, 它计算图像像素直方图, 而与图像像素的空间位置排列无关.

4 本文方法实现流程

基于 Haar 小波域指标自适应选择载体的 JPEG 隐写的实现框架如图 2 所示.

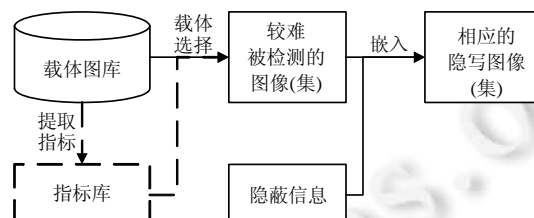


Fig.2 Implementation framework of JPEG steganography based on adaptive cover selection

图 2 自适应选择载体的 JPEG 隐写实现框架

传统的多样本隐写方法(图 2 实线部分)通常将消息进行分片, 顺序或随机地从图像库中选用一部分图像用于嵌入. 而本文载体选择的隐写方法在传统隐写方法基础上增加了提取指标及载体选择环节(图 2 虚线部分). 具体步骤如下.

- (1) 从载体图像库中随机选择 N 幅图像作为待发送的图像.
- (2) 在隐写算法实施之前, 对选中的每个图像做 Haar 小波变换, 并根据公式(1)计算 Haar 小波域指标值.
- (3) 将所计算的指标值按照降序排列.
- (4) 优先选择在指标值排名靠前的图像进行隐写嵌入, 直至消息嵌入完成. 如果不足, 则选择更多的图像;

(5) 将所选择的待发送图像(包括隐写和未隐写图像)一起传输,避免传输过多纹理丰富的图像引起怀疑.

在多样本隐写的具体实现并非所有图像都参与了隐写,发送方在发送信息时对隐蔽消息的分片加入固定格式,如:依次嵌入消息长度、分片偏移量、消息数据、校验码.接收方在提取信息时,如果校验错误则放弃解码.

本文方法有如下优点:第一,通过计算指标选择载体,避免大量计算影响用户体验;第二,纹理丰富的图像较难检测是普遍规律,兼容现有的大多数隐写算法;第三,解码端不需要较大的改动,便于使用.

5 实验

5.1 实验条件与评价指标

本文选用公开图像库 BOSSv0.92(10 074 张,512×512 像素)和 BOSSv1.01(10 000 张,从 BOSSv1.01 图库 RAW 格式等比例缩小至 512 像素×768 像素).从图像库每次随机选取 1 000 张图像用于测试,其余 9 000(BOSSv0.92 为 9 074)张用于训练.图像使用隐写算法得到隐写图像,提取特征并用训练和测试,得到 1 000 对测试结果.同时,计算 1 000 幅测试图像的各种纹理复杂度指标.在仿真嵌入时,选用在 JPEG 量化系数非自适应的 nsF5 算法和在边信息内容自适应的 SI-UNIWARD 算法.实验所用 JPEG 质量因子为 85.隐写分析使用目前最为有效的高维 JPEG 特征之一:CC-JRM 特征和 DCTR 特征^[20],对应的分类器是组合 FLD 分类器.实验还测试了空域隐写下的情况,选用目前较难检测的 MiPOD 和 S-UNIWARD 隐写方法以及最为有效的 MaxSRM 特征^[21].

本文评价图像纹理度量与该类图像用于隐写分析的准确率值二者之间的关系,主要选用相关性指标和准确率两种评价指标.

(1) 相关性指标

计算图像纹理度量与隐蔽性之间的 Spearman 秩相关系数^[12]:

$$\rho(X, Y) = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}} \quad (2)$$

其中, x_i, y_i 分别为 X, Y 中第 i 个元素 X_i, Y_i 的次序, \bar{x}, \bar{y} 分别为 x_i 和 y_i 的均值.在实验时, X 为图像纹理度量组成的向量, Y 为图像隐蔽性构成的向量, Y_i 表示第 i 幅载体图像及对应隐写图像在隐写分析时正确预测的次数. Spearman 秩相关系数绝对值较大的纹理评价指标与该图像用于隐写时的隐蔽性相关性较大,用其优选出纹理复杂度高的图像,同时也能较为准确地优选出隐写隐蔽性较强的图像.

(2) 隐蔽性指标

将图像按照纹理度量排序,优先选择排名靠前的若干幅载体图像后,统计该部分图像的载体及对应隐写图像在隐写分析时的准确率.该指标相对直观,能够从优选后准确率变化比较各种图像纹理度量的优劣.同样比例下优选载体时,隐写分析准确率越低的隐蔽性越好.在优选的图像数量上升过程中,优选图像数量与隐写分析准确率关系曲线抖动越小,隐蔽性越好.

5.2 载体选择指标的相关性检验

为了验证本文方法的有效性,本节以公开图像库为例计算图像纹理指标与隐蔽性之间的 Spearman 秩相关系数,并与信息熵、LPE 和 LV 等指标做对比.实验对每一对测试图像计算图像纹理指标组成向量 X ,并计算分类器对这一对图像预测结果的正确次数组成向量 Y .将两组向量代入公式(2)即得到 Spearman 秩相关系数.本文 Haar 小波域纹理指标在不同参数下与隐蔽性的 Spearman 秩相关系数实验的结果见表 1.表中主要列举在 nsF5 0.10 bpac, SI-UNIWARD 0.70 bpac 和 0.90 bpac 下,参数 k, r 和 Haar 小波算法在公式(1)的 H(水平)、V(竖直)、D(对角线)和它们的均值(表中标注为均值)作为指标时的 Spearman 秩相关系数.

从表中可以看出,在不同情况下,各分量的相关系数有高低差别,但均值指标比 HVD 各分量更稳定.当 $k=3, r=1$ 时,小波系数 H, V 和 D 的均值作为指标时, Spearman 相关系数值总体较高,即隐蔽性受指标影响较大,这样的指标用于载体选择更能有效地优选难检测的载体.

Table 1 Spearman correlation coefficients of each component of proposed indicators under different JPEG steganography algorithms

表 1 在不同 JPEG 隐写算法下,本文指标各组成成分的 Spearman 相关系数

K	r	nsF5 0.10 bpac				SIUW 0.70 bpac				SIUW 0.90 bpac			
		H	V	D	均值	H	V	D	均值	H	V	D	均值
1	1	0.22	0.23	0.24	0.23	-0.02	-0.04	-0.01	-0.02	0.16	0.17	0.20	0.18
1	2	0.20	0.22	0.20	0.21	0.00	-0.01	0.00	-0.01	0.18	0.21	0.21	0.20
1	3	0.18	0.20	0.18	0.19	0.00	0.00	0.01	0.00	0.18	0.22	0.21	0.21
2	1	0.22	0.23	0.23	0.23	0.01	0.00	0.03	0.01	0.18	0.20	0.21	0.20
2	2	0.20	0.22	0.19	0.20	0.03	0.02	0.03	0.03	0.18	0.23	0.21	0.21
2	3	0.17	0.21	0.16	0.18	0.03	0.03	0.03	0.03	0.17	0.23	0.20	0.20
3	1	0.21	0.23	0.21	0.22	0.05	0.05	0.06	0.05	0.18	0.23	0.21	0.21
3	2	0.18	0.21	0.17	0.19	0.05	0.06	0.05	0.05	0.17	0.24	0.20	0.21
3	3	0.15	0.19	0.15	0.17	0.05	0.07	0.05	0.05	0.15	0.23	0.19	0.19

为比较本文方法与已有方法的有效性,实验随机选取了 BOSS v1.01 图像库及其对应隐写图像分别提取了信息熵(标记为 Ent.)、LPE 1、LPE 2 和 LV 指标.实验同时计算了 Matlab 中常见的几种小波,检验其他小波特征也具有类似的效果.结果见表 2,其中,第 4 列~第 8 列列举出不同指标下的载体选择指标与隐蔽性相关系数.从表中可以看出,本文方法指标值在相关性方面普遍高于同比的指标,实验统计了 BOSS v0.92 和 BOSS v1.01 图像库下,对 nsF5 0.05~0.20 bpac 和 SI-UNIWARD 0.70~0.90 bpac 的情况,本文方法比信息熵、LPE 1、LPE 2、LV 方法的相关系数平均高约 0.032,比已有方法中最优的 LPE1 高约 0.021.

Table 2 Spearman correlation coefficients of different indicators under different JPEG steganography algorithms (BOSSv1.01 image database)

表 2 在不同 JPEG 隐写下,不同指标的 Spearman 相关系数(BOSSv1.01 图像库)

隐写特征	隐写算法	嵌入率 bpac	Ent.	LPE 1	LPE 2	LV	HAAR	BIOR 4.4	COIF3	DB8	RBIO 4.4	SYM8
CC-JRM	nsF5	0.05	0.093	0.104	0.104	0.095	0.115	0.120	0.118	0.117	0.117	0.114
		0.10	0.142	0.154	0.152	0.138	0.169	0.172	0.170	0.168	0.170	0.161
		0.20	0.155	0.121	0.120	0.110	0.151	0.150	0.151	0.148	0.150	0.149
	SI-UW	0.70	0.051	0.025	0.021	0.040	0.073	0.060	0.060	0.062	0.066	0.049
		0.90	0.122	0.146	0.142	0.157	0.172	0.168	0.168	0.169	0.171	0.158
DCTR	nsF5	0.05	0.062	0.053	0.049	0.048	0.060	0.051	0.051	0.051	0.052	0.051
		0.10	0.121	0.102	0.098	0.097	0.120	0.109	0.109	0.109	0.111	0.109
		0.20	0.120	0.112	0.111	0.095	0.120	0.113	0.112	0.112	0.114	0.112
	SI-UW	0.70	0.161	0.196	0.190	0.200	0.199	0.183	0.184	0.184	0.187	0.184
		0.90	0.158	0.190	0.187	0.193	0.194	0.183	0.183	0.184	0.186	0.183

实验还测评了当前较难检测的空域隐写算法及其参数下的 Spearman 秩相关系数.实验随机选取了 BOSSv0.92 图像库,分别提取了与表 2 实验同样的指标.唯一不同的是空域情形下,通过遍历得出在 $k=1, r=1$ 时指标的有效性较好,因而空域实验选取该组参数.实验结果见表 3.对比表 2 和表 3 可以看出,空域隐写算法对不同纹理复杂度的图像表现不同,其与 JPEG 隐写算法相比更依赖于图像的纹理复杂度,即主要表现为相关系数明显增大.从表 3 可以看出,空域隐写下,小波域系数在大多数情况下略高于已有指标.可以得出结论,本文指标载体优选方法对提高空域隐写算法隐蔽性有一定的作用,但提高的效果不如 JPEG 算法.

Table 3 Absolute value of Spearman correlation coefficients of different indicators under different spatial steganography algorithms (BOSSv0.92 image database)

表 3 在空域隐写算法下不同指标的 Spearman 相关系数绝对值(BOSSv0.92 图像库)

隐写算法	嵌入率 bpac	Ent.	LPE 1	LPE 2	LV	HAAR	BIOR4.4	COIF3	DB8	RBIO4.4	SYM8
MiPOD	0.10	0.186	0.352	0.357	0.312	0.356	0.375	0.374	0.372	0.371	0.373
	0.30	0.191	0.369	0.374	0.323	0.371	0.392	0.390	0.388	0.388	0.390
	0.50	0.187	0.328	0.331	0.296	0.335	0.344	0.344	0.342	0.342	0.343
S-UW	0.30	0.283	0.548	0.552	0.474	0.562	0.586	0.584	0.579	0.579	0.583
	0.50	0.272	0.544	0.545	0.476	0.563	0.579	0.577	0.573	0.574	0.577

5.3 不同小波算法下的相关性检验

为了测试不同小波算法的有效性,实验还在 Matlab 中比较不同小波基的情况下,指标值与隐写分析检测率的 Spearman 相关性情况.如表 2 和表 3 所示,选用的小波包括 Haar 小波(标记为 HAAR)、双正交小波(低通滤波器、重建滤波器阶数为 4,标记为 BIOR 4.4)、Coiflets 小波(3 阶,标记为 COIF 3)、反正交小波(低通滤波器、重建滤波器阶数为 4,标记为 RBIO 4.4)、Daubechies 小波(8 阶,标记为 DB 8)、Symlets 小波(8 阶,标记为 SYM 8).表 2 最右 6 列列举了不同隐写算法和嵌入率下的结果.实验结果表明,同等情况下,Haar 小波的相关系数与表中其他小波基相近.但 Haar 小波实现方法简单,更具优势.在空域隐写方面,如表 3 所示,Haar 小波的表现也相近.

5.4 载体选择效果对照

实验还从隐蔽性指标方面比较了本文方法与同类方法在载体选择上的有效性.先对 1 000 幅待测图像按给定统计指标排序,选择指标最小(当指标与隐写隐蔽性呈负相关时)或最大(当指标与隐写隐蔽性呈正相关时)的前 N 幅图像,统计隐写分析对该部分载体图像及其对应隐写图像的准确率.图 3 展示了使用 BOSS v1.01 图库在 nsF5 0.05 bpac 和 SIUW 0.90 bpac 隐写时,随机选择 N 幅图、根据图像熵(Ent)、LPE1、LV 和本文方法等准则优选 N 幅图时, N 随隐蔽性变化情况.此时,使用的是 CCJRM 特征.相应地,图 4 展示了使用 BOSS v0.92 图库在 nsF5 0.20 bpac 和 SIUW 0.80 bpac 隐写时, N 随隐蔽性变化情况.此时,使用的是 DCTR 特征.

从图 3 和图 4 中可以看出,大多数情况下,本文方法指标优选出的图像隐蔽性较高,而且本文指标优选的优势较为稳定.以图 4 中 $N=60$ 处为例,在 SIUW 隐写嵌入率 0.80 bpac 的情况下,从给定的测试图像集中选择 60 幅图像用于隐写,隐写分析的平均错误率约为 5.1%.使用载体选择的隐写方法可以提升这一指标,信息熵、LV 和 LPE1 方法提高至 10.9%~12.4%,而本文 Haar 小波域指标将隐蔽性提升至 15.9%.这一优势总体存在,直至 N 已接近样本总量的一半.除了在优选载体数量 N 较小时统计不够稳定之外,在相同数量下,本文方法优选的图像隐蔽性优于已有算法.而且,本文指标的曲线与其他指标的曲线相比,下降趋势更稳定,抖动较少.相反地,抖动较多的曲线即使在个别区域得到较高的隐蔽性,但下降过程不稳定,实用中很难准确地把握优选载体的数量.

从图中还可看出,随着 N 增大,隐蔽性越来越高,本文方法与隐蔽性间的递增关系相对明显.这与 Spearman 相关系数指标相印证,即相关系数高的方法在载体选择上表现更好.实验统计了 BOSS v0.92 和 BOSS v1.01 图像库下,对 nsF5 0.05~0.20 bpac 和 SI-UNIWARD 0.70~0.90 bpac 优选 50~100 幅图像的载体选择效果,本文方法比信息熵、LPE 1、LPE 2 和 LV 方法的隐蔽性平均低约 2.4%,比已有方法中最优者(LV)低约 1.7%,比随机选择(即不进行优选)平均低约 7.8%.可以认为,本文选择载体的方法进一步提高了现有高隐蔽性隐写算法的隐蔽性.

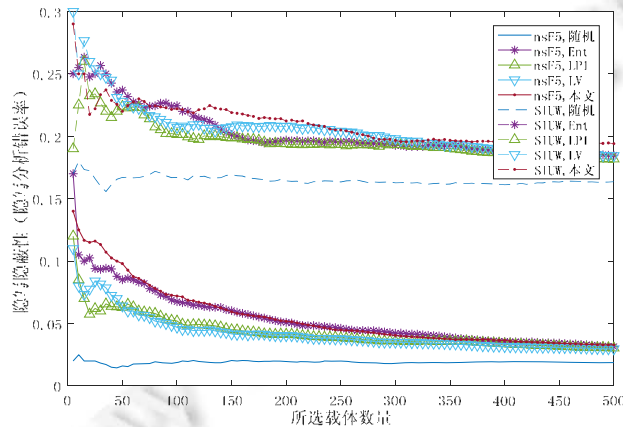


Fig.3 Comparison of the relations of the selected image amount and steganalysis error rate using different JPEG steganography cover selection indicators (nsF5 0.05 bpac, SIUW 0.90 bpac)

图 3 不同指标进行 JPEG 隐写载体选择数量与隐写分析错误率关系比较(nsF5 0.05 bpac,SIUW 0.90 bpac)

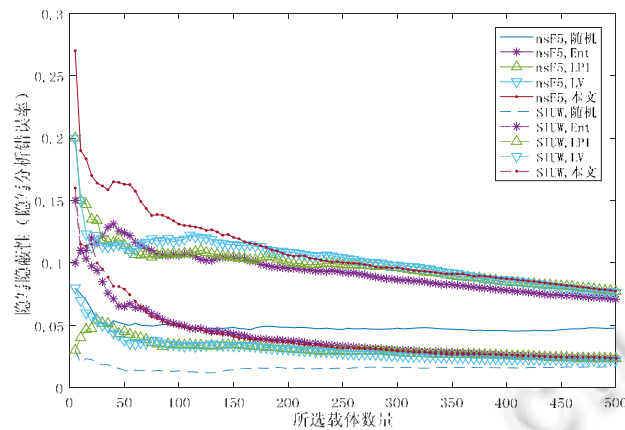


Fig.4 Comparison of the relations of the selected image amount and steganalysis error rate using different JPEG steganography cover selection indicators (nsF5 0.20 bpac, SIUW 0.80 bpac)

图 4 不同指标进行 JPEG 隐写载体选择数量与隐写分析错误率关系比较(nsF5 0.20 bpac,SIUW 0.80 bpac)

6 总 结

本文提出了一种基于 Haar 小波域指标自适应选择载体的 JPEG 隐写.该指标通过计算图像在 Haar 小波域的高频成分分解图像的高阶范数,用以优选 JPEG 隐写的载体图像.隐写者可以在隐写之前利用该指标预先筛选出难以检测的图像,在一定程度上增加了隐写分析者的困难,即提高了隐写行为的隐蔽性.实验结果表明,本文方法提高了隐写行为的隐蔽性,效果比现有的基于图像纹理评价的载体选择指标更优.我们基本达到了研究目的,但仍存在着一些不足,如所选用的指标模型较为简单,在 Spearman 相关系数或载体选择的效果等方面都低于空域隐写,尚有提升空间,以及本文的结论是否对构造隐写分析的训练集有所帮助,这些都是下一步研究需要解决的问题.

References:

- [1] Cachin C. An information-theoretic model for steganography. In: Aucsmith D, ed. Proc. of the 2nd Int'l Workshop on Information Hiding (IH'98). Berlin, Heidelberg: Springer-Verlag, 1998. 306–318.
- [2] Fridrich J, Kodovský J. Rich models for steganalysis of digital images. IEEE Trans on Information Forensics and Security, 2012, 7(3):868–882.
- [3] Pevný T, Fridrich J. Benchmarking for steganography. In: Solanki K, Sullivan K, Madhow U, eds. Proc. of the 10th Int'l Workshop on Information Hiding (IH 2008). Berlin, Heidelberg: Springer-Verlag, 2008. 251–267.
- [4] Ker AD, Bas P, Böhme R, Congranne R, Craver S, Filler T, Fridrich J, Pevný T. Moving steganography and steganalysis from the laboratory into the real world. In: Proc. of the 1st ACM Workshop on Information Hiding and Multimedia Security. 2013. 45–58.
- [5] Kim Y, Duric Z, Richards D: Modified matrix encoding technique for minimal distortion steganography. In: Camenisch JL, Collberg CS, Johnson NF, Sallee P, eds. Proc. of the 8th Int'l Workshop on Information Hiding (IH 2006). Berlin, Heidelberg: Springer-Verlag, 2007. 314–327.
- [6] Fridrich J, Pevný T, Kodovský J. Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities. In: Proc. of the 9th Workshop on Multimedia & Security. 2007. 3–14.
- [7] Filler T, Judas J, Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans. on Information Forensics and Security, 2011,6(3):920–935.
- [8] Holub V, Fridrich J, Denmark T. Universal distortion function for steganography in an arbitrary domain. EURASIP Journal on Information Security, 2014,2014(1):1–13.

- [9] Sedighi V, Cograne R, Fridrich J. Content-Adaptive steganography by minimizing statistical detectability. *IEEE Trans. on Information Forensics and Security*, 2016,11(2):221–234.
- [10] Kodovský J, Fridrich J. Steganalysis of JPEG images using rich models. In: *Proc. of the SPIE 8303, Media Watermarking, Security, and Forensics 2012*. 2012. No.83030A.
- [11] Pevný T, Fridrich J. Merging Markov and DCT features for multi-class JPEG steganalysis. In: *Proc. of the SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX*. 2007. No.650503.
- [12] Böhme R. Assessment of steganalytic methods using multiple regression models. In: Barni M, Herrera-Joancomartí J, Katzenbeisser S, Pérez-González F, eds. *Proc. of the 7th Int'l Workshop on Information Hiding (IH 2005)*. Berlin, Heidelberg: Springer-Verlag, 2005. 278–295.
- [13] Kharrazi M, Sencar HT, Memon N. Cover selection for steganographic embedding. In: *Proc. of the Int'l Conf. on Image Processing 2006*. IEEE, 2006. 117–120.
- [14] Gul G, Kurugollu F: A new methodology in steganalysis: breaking highly undetectable steganography (HUGO). In: Filler T, Pevný T, Craver S, Ker A, eds. *Proc. of the 13th Int'l Conf. on Information Hiding (IH 2011)*. Berlin, Heidelberg: Springer-Verlag, 2011. 71–84.
- [15] Huang W, Zhao X. Novel cover selection criterion for spatial steganography using linear pixel prediction error. *Science China Information Sciences*, 2016,59(5):No.059103.
- [16] Huang W, Zhao X. Reliable pooled steganalysis using fine-grained parameter estimation and hypothesis testing. In: Shi YQ, Kim HJ, Perez-Gonzalez F, Liu F, eds. *Proc. of the 15th Int'l Workshop on Digital Forensics and Watermarking (IWDW 2016)*. Cham: Springer-Verlag, 2017. 550–563.
- [17] Kouider S, Chaumont M, Puech W. Technical points about adaptive steganography by oracle (ASO). In: *Proc. of the 20th European Signal Processing Conf. (EUSIPCO)*. 2012. 1703–1707.
- [18] Sajedi H, Jamzad M. Secure cover selection steganography. In: Park JH, Chen HH, Atiquzzaman M, Lee C, Kim TH, Yeo SS, eds. *Proc. of the 3rd Int'l Conf. and Workshops on Advances in Information Security and Assurance (ISA 2009)*. Berlin, Heidelberg: Springer-Verlag, 2009. 317–326.
- [19] Sajedi H, Jamzad M. Using contourlet transform and cover selection for secure steganography. *Int'l Journal of Information Security*, 2010,9(5):337–352.
- [20] Holub V, Fridrich J. Low-Complexity features for JPEG steganalysis using undecimated DCT. *IEEE Trans. on Information Forensics and Security*, 2015,10(2):219–228.
- [21] Denmark T, Sedighi V, Holub V, *et al.* Selection-Channel-Aware rich model for steganalysis of digital images. In: *Proc. of the 2014 IEEE Int'l Workshop on Information Forensics and Security (WIFS)*. 2014. 48–53.



黄炜(1985—),男,福建南安人,博士,助理教授,主要研究领域为信息隐藏.



赵险峰(1969—),男,博士,研究员,博士生导师,CCF 专业会员,主要研究领域为信息隐藏.