



JOURNAL OF IMAGE AND GRAPHICS

主办: 中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象学报 中国图形学报

2014

09

VOL.19

ISSN1006-8961
CN11-3758/TB





第19卷第9期 (总第221期)

2014年9月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊

版权声明

凡向《中国图象图形学报》投稿, 均视为同意在本刊网站及CNKI等全文数据库出版, 所刊载论文已获得著作权人的授权。本刊所有图片均为非商业目的使用, 所有内容, 未经许可, 不得转载或以其他方式使用。

Copyright

All rights reserved by Journal of Image and Graphics, Institute of Remote Sensing and Digital Earth, CAS. The content (including but not limited text, photo, etc) published in this journal is for non-commercial use.

主管单位 中国科学院

主办单位 中国科学院遥感与数字地球研究所

中国图象图形学学会

北京应用物理与计算数学研究所

主 编 李小文

编辑出版 《中国图象图形学报》编辑出版委员会

邮政信箱 北京9718信箱

邮 编 100101

电子信箱 jig@irsa.ac.cn

电 话 010-64807995

网 址 www.cjig.cn

广告经营许可证 京朝工商广字第0361号

总 发 行 北京报刊发行局

订 购 全国各地邮局

海外发行 中国国际图书贸易集团有限公司

(邮政信箱: 北京399信箱 邮编: 100048)

印刷装订 北京科信印刷有限公司

Journal of Image and Graphics

Title inscription: Song Jian

Monthly, Started in 1996

Superintended by Chinese Academy of Sciences

Sponsored by Institute of Remote Sensing and Digital Earth, CAS

China Society of Image and Graphics

Institute of Applied Physics and Computational Mathematics

Editor-in-Chief LI Xiaowen

Editor, Publisher Editorial and Publishing Board of Journal of
Image and Graphics

P.O.Box 9718, Beijing, P.R.China

Zip code 100101

E-mail jig@irsa.ac.cn

Telephone 010-64807995

Website www.cjig.cn

Distributed by Beijing Bureau for Distribution of Newspapers and Journals

Domestic All Local Post Offices in China

Overseas China International Book Trading Corporation

(P.O.Box 399, Beijing 100048, P.R.China)

Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB

ISSN 1006-8961

CODEN ZTTXFZ

国外发行代号 M1406

国内邮发代号 82-831

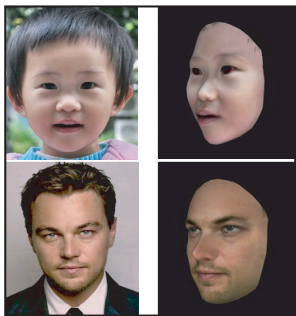
国内定价 50.00元



自适应对称自回归模型的压缩图像内插方法(第1268页)



加权局部特征结合判别式字典的目标跟踪算法(第1316页)



结合特征适配与拉普拉斯形变的3维人脸重建(第1349页)

综述

能量泛函正则化模型在图像恢复中的应用分析

李旭超, 刘海宽, 宋博 1247

图像处理和编码

融合最小化失真与模型保持的隐写算法

高瞻瞻, 汤光明, 张伟伟 1260

自适应对称自回归模型的压缩图像内插方法

刘婧, 干宗良, 崔子冠, 陈昌红, 朱秀昌 1268

基于能量泛函和视觉特性的全变分图像降噪模型

郭从洲, 秦志远, 时文俊 1282

分块策略实现图像椒盐噪声密度估计

林亚明, 李佐勇, 林叶郁 1288

图像分析和识别

Dempster-Shafer证据融合金字塔韦伯局部特征的表情识别

王晓华, 金超, 任福继, 胡敏 1297

运动捕捉数据中足迹的谱聚类检测方法

刘晓平, 陆劲挺, 谢文军 1306

加权局部特征结合判别式字典的目标跟踪

王飞, 房胜 1316

面向瓦当文字识别的改进水平集骨架提取

邓茜芸, 周明全, 武仲科, 王醒策 1324

改进复杂网络模型的形状特征提取

阮瑞, 江波, 汤进, 罗斌 1332

几何特性二元关系的直线匹配

胡海霞, 李钢 1338

图像理解和计算机视觉

结合特征适配与拉普拉斯形变的3维人脸重建

张剑, 何骅, 詹小四, 肖俊 1349

利用背景加权和选择性子模型更新的视觉跟踪算法

黄安奇, 侯志强, 余旺盛, 刘翔 1360

计算机图形学

对可控Bézier曲线的改进

严兰兰, 韩旭里 1368

医学图像处理

结合区域生长与灰度重建的CT图像肺气管树分割

彭双, 肖昌炎 1377

检测肺结节的3维自适应模板匹配

高婷, 龚敬, 王远军, 聂生东, 孙希文 1384

CONTENTS

JOURNAL OF IMAGE AND GRAPHICS



Novel compression image interpolation method using adaptive symmetrical autoregressive models(P1268)



Visual tracking based on discriminative dictionary and weighted local features (P1316)



Three dimensional face reconstruction via feature adaptation and Laplace deformation (P1349)

Review

- Application analysis of regularization model of energy functional to image restoration
Li Xuchao, Liu Haikuan, Song Bo 1247

Image Processing and Coding

- Steganographic method combining minimum embedding distortion and model preservation
Gao Zhanzhan, Tang Guangming, Zhang Weiwei 1260
- Novel compression image interpolation method using adaptive symmetrical autoregressive models
Liu Jing, Gan Zongliang, Cui Ziguang, Chen Changhong, Zhu Xiuchang 1268
- TV image denoising model based on energy functionals and HVS
Guo Congzhou, Qin Zhiyuan, Shi Wenjun 1282
- Image salt-and-pepper noise estimation based on partitioning strategy
Lin Yaming, Li Zuoyong, Lin Yeyu 1288

Image Analysis and Recognition

- Research on facial expression recognition based on pyramid Weber local descriptor and the Dempster-Shafer theory of evidence
Wang Xiaohua, Jin Chao, Ren Fuji, Hu Min 1297
- Foot plant detection based on spectral clustering algorithm for motion capture data
Liu Xiaoping, Lu Jintong, Xie Wenjun 1306
- Visual tracking based on the discriminative dictionary and weighted local features
Wang Fei, Fang Sheng 1316
- Skeleton extraction using improved level set methods in eaves' text recognition
Deng Qianyun, Zhou Mingquan, Wu Zhongke, Wang Xingce 1324
- Improved shape feature extraction using complex network model
Ruan Rui, Jiang Bo, Tang Jin, Luo Bin 1332
- Line matching based on binary relations of geometric attributes
Hu Haixia, Li Gang 1338

Image Understanding and Computer Vision

- Three dimensional face reconstruction via feature adaptation and Laplace deformation
Zhang Jian, He Hua, Zhan Xiaosi, Xiao Jun 1349
- Visual object tracking method based on weighted background and selective sub-model update strategy
Huang Anqi, Hou Zhiqiang, Yu Wangsheng, Liu Xiang 1360

Computer Graphics

- Improvement of the modifiable Bézier curves
Yan Lanlan, Han Xuli 1368

Medical Image Processing

- Segmentation of pulmonary airway tree in CT images by combining region growing and grayscale reconstruction algorithms
Peng Shuang, Xiao Changyan 1377
- Three dimensional adaptive template matching algorithm for lung nodule detection
Gao Ting, Gong Jing, Wang Yuanjun, Nie Shengdong, Sun Xiwen 1384

中图法分类号: TP309 文献标识码: A 文章编号: 1006-8961(2014)09-1260-08

论文引用格式: Gao Z Z, Tang G M, Zhang W W. Steganographic method combining minimum embedding distortion and model preservation[J]. Journal of Image and Graphics, 2014, 19(9): 1260-1267. [高瞻瞻, 汤光明, 张伟伟. 融合最小化失真与模型保持的隐写算法[J]. 中国图象图形学报, 2014, 19(9): 1260-1267.] [DOI: 10. 11834/jig. 20140902]

融合最小化失真与模型保持的隐写算法

高瞻瞻, 汤光明, 张伟伟

解放军信息工程大学, 郑州 450001

摘要: **目的** 为了保证载密图像的抗统计分析能力同时避免对特定载体模型的过度优化, 提出一种以最小化失真为目标的隐写算法。 **方法** 算法以各方向元素基团为基本单元定义失真函数, 以 Fisher 准则函数的极大值为标准对失真参数进行优化, 将失真函数与统计特征相关联。在秘密信息的嵌入过程中, 首先依据邻域系统将图像载体分为若干元素阵列, 令不同的阵列对应不同的特征子集, 再利用 Gibbs 抽样和 STC (Syndrome-trellis code) 编码实现对这些有所差异的特征子集的集成, 从而在最小化失真的同时保持载体的统计特征。 **结果** 在 3 组不同维数的检测算法下比较该算法与同类算法的分类误差。结果表明, 该算法能更好地保持统计模型, 嵌入率为 0.5 bit/pixel 时相应特征集的检测误差仍高于 0.4, 面临高维检测时算法同样具有较高的安全性。 **结论** 该算法借助最小失真思想实现了隐写前后统计特征的保持, 且有效避免了在不完整模型上的过度优化, 拥有比同类算法更好的适应性和安全性。

关键词: 隐写术; Gibbs 随机场; 失真函数; 特征分析

Steganographic method combining minimum embedding distortion and model preservation

Gao Zhanzhan, Tang Guangming, Zhang Weiwei

PLA Information and Technology University, Zhengzhou 450001, China

Abstract: **Objective** The development of steganalysis technology, especially universal blind steganalysis based on statistical characteristics, has increased the demand for steganographic security against statistical analysis. To ensure stego-image security against statistical analysis while avoiding overtraining to an incomplete cover model, this study presents a steganographic method that minimizes embedding distortion. **Method** A novel distortion function reflecting higher order statistics is first defined based on element cliques. According to the results of theoretical derivation and experiments, the maximal value of the Fisher criterion function is used as the optimization criterion for the parameters in the distortion function, such that the distortion function can be related to statistical detectability. Finally, when a secret message is embedded, multiple different feature subsets are integrated through Gibbs sampling and syndrome-trellis coding. Statistical characteristics are preserved while distortion is minimizes. **Result** Experiments are proposed to compare the classification errors of the new method with those of three similar steganalysis methods with different dimensions. Results show that the new method can better preserve image model and maintains high security even when detected using a high-dimensional steganalysis method. The classification error using corresponding feature set is higher than 0.4 while the embedding rate is 0.5 bit/pixel. **Conclusion** The new steganographic method successfully preserves statistical characteristics while minimizing distortion function.

收稿日期: 2013-12-18; 修回日期: 2014-05-04

基金项目: 国家自然科学基金项目 (61101112); 河南省科技攻关基金项目 (122102210047)

第一作者简介: 高瞻瞻 (1988—), 男, 解放军信息工程大学博士研究生, 主要研究方向为隐写术、隐写分析。E-mail: gaozhanyx@

Moreover, the proposed steganographic method effectively avoids overtraining to an incomplete model and has better adaptability and security than similar methods.

Key words: steganography; Gibbs random field; distortion function; feature analysis

0 引言

隐写是一种将秘密信息存储到图像、音频、视频等常见载体中以实现隐蔽通信的技术。目前,隐写算法的研究主要针对图像载体,其设计思想大体可以归为以下两类。

第1类隐写算法以最小化嵌入影响为目标。以STC编码^[1]为代表的隐写编码技术的发展,使该类算法的设计日趋成熟^[2-3],也使得该类算法的研究重心转变为失真函数的定义。但是,由于目前的编码方法尚不能在嵌入时最小化一般形式的失真函数,该类算法长期局限在载体元素的加性失真这一特殊形式下,无法反映嵌入改变间的影响。为了弥补这一不足,文献[4]提出Gibbs构造隐写算法,以元素基团为基本单元定义失真函数,但在具体应用时其定义只反映了相邻两元素间的关系。

另一类算法以载体模型保持为基本思想。目前,这类隐写往往仅能考虑图像某一方面的特征而忽略其他特征,这使其安全性无法得到保证。如Agaian^[5]提出的方法和Lou等人^[6]提出的基于局部复杂度的自适应隐写算法,这些方法虽然能够抵御针对一阶直方图的攻击,但高阶统计失真明显。张湛等人^[7]基于隐写编码和图像Markov链模型的隐写方法也只做到了二阶统计特性的保持。此外,文献[8]利用相邻像素差分设计失真函数,基于编码嵌入机制设计的隐写算法也只是针对的SPAM特征检测。文献[9]指出,按照某一模型过度优化的自适应隐写虽然可以有效抵抗该模型范围内的特征检测,但攻击者采用模型外的特征时可能得到非常准确的检测结果,如FCM算法^[10]。文献[11]的实验结果表明,对于各类检测普适能力较强的JPEG隐写算法依然是早期的非自适应算法nsF5。

本文尝试一种通用的模型保持隐写算法,能够避免对特定特征集的过度优化并且可以适用于新的隐写特征和新的图像。在文献[4]的基础上,利用水平方向、垂直方向、对角方向的元素基团给出了失真D的一种特殊的加性和形式,使失真定义包含更高阶的统计特征。通过失真参数的优化将D与载

体和载密体特征向量间的差异相关联,再利用Gibbs抽样理论实现信息的嵌入,从而在最小化嵌入失真的同时保持了载体统计特征。

1 载密体的最优分布

用 $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbf{I}^n$ 表示载体图像, $\mathbf{I}$ 表示载体元素的取值空间。用 $\mathbf{Y}$ 表示载体 $\mathbf{x}$ 嵌入信息后所有可能的载密体构成的集合。载密体用变量 Y 表示,其取值是 $\mathbf{Y}$ 上的概率分布, $P(Y = y) = \varphi(y), y \in \mathbf{Y}$ 。当秘密信息比特数 m 确定时,最优隐写应既能保证所需的嵌入量,又具有最小的嵌入失真,即

$$\begin{cases} \text{minimize } E_{\varphi}[D] = \sum_{y \in \mathbf{Y}} \varphi(y) D(y) \\ \text{s. t. } H(\varphi) = - \sum_{y \in \mathbf{Y}} \varphi(y) \log \varphi(y) = m \end{cases} \quad (1)$$

满足式(1)的载密体最优分布具有Gibbs形式^[4],即

$$\varphi_{\lambda}(y) = \frac{\exp(-\lambda D(y))}{Z(\lambda)} \quad (2)$$

式中, $Z(\lambda)$ 是归一化因子,即

$$Z(\lambda) = \sum_{y \in \mathbf{Y}} \exp(-\lambda D(y))$$

λ 的值由式(1)的限制条件决定。

要得到具有最小失真的载密体,实现信息的最优嵌入,隐写算法需要找到服从最优分布 φ_{λ} 的一个样本。通过Gibbs抽样可以实现这一目的。为了说明其抽样原理,在集合 $\mathbf{Y}$ 上定义转移概率矩阵

$$\tilde{\mathbf{O}}_i(y, y') = \begin{cases} \varphi_{\lambda}(Y_i = y'_i | Y_{-i} = y_{-i}) & Y_{-i} = y'_{-i} \\ 0 & \text{其他} \end{cases}$$

$$\varphi_{\lambda}(Y_i = y'_i | Y_{-i} = y_{-i}) = \frac{\pi_{\lambda}(y'_i y_{-i})}{\sum_{t_i \in I_i} \pi_{\lambda}(t_i y_{-i})} \quad (3)$$

式中, $\varphi_{\lambda}(Y_i = y'_i | Y_{-i} = y_{-i})$ 表示其他载体元素不变,元素 y_i 变为 y'_i 的条件概率。

Gibbs抽样包含多次扫描(sweep)过程,每次扫描都按访问序列 σ 遍历所有元素,计算其局部转移概率 $\tilde{\mathbf{O}}_{\sigma(i)}(y'_{\sigma(i)} y_{-\sigma(i)}, y)$, $y'_{\sigma(i)} \in \mathbf{I}_{\sigma(i)}$,并根据该概率从 $\mathbf{I}_{\sigma(i)}$ 中随机取值以修改 $y_{\sigma(i)}$ 。可见,矩阵 $\tilde{\mathbf{O}}_{\sigma}$ 对应了一个不可约的Markov过程。用符号 $\psi_{\lambda} \in$

$[0, \infty)^{|Y|}$ 表示含有 $|Y|$ 个非负元素的向量, $\psi_\lambda = \varphi_\lambda(y), y \in Y$, 则 ψ_λ 是矩阵 $\tilde{D}_\sigma$ 的左特征向量及其稳定分布^[4]。根据 Markov 链理论, 对于不可约的 Markov 链 $\tilde{D}_\sigma$, 不论最初的嵌入改变 $\tau \in [0, \infty)^{|Y|}$ 是怎样的分布, 随着扫描次数的增加, Gibbs 抽样样本的分布将趋向于 ψ_λ 。这意味着, 通过重复运行扫描过程就可以得到服从最优分布 φ_λ 的样本。

2 失真函数的定义

定义 1^[12] 称 $\eta = \{\eta(i) | i \in \kappa\}$ 是定义在图像索引集 $\kappa = \{1, 2, \dots, n\}$ 上的邻域系统, 若 η 满足以下特性: 1) $\eta(i) \subset \kappa$, 2) $i \notin \eta(i)$, 3) $\forall i, j \in \kappa, i \in \eta(j) \Leftrightarrow j \in \eta(i)$ 。 $\eta(i)$ 中的元素称为元素 i 的相邻元素。

依据邻域系统 η 可以将图像载体元素划分为若干阵列, 使不同阵列中的元素不构成相邻关系。二阶邻域系统下的图像 x (分辨率为 $n_1 \times n_2$) 可以划分为 4 个元素阵列, 即

$$\begin{aligned} \kappa &= \bigcup_{st} \kappa_{st}, 1 \leq s, t \leq 2 \\ \kappa_{st} &= \{(s+2l, t+2l') | 1 \leq s+2l \leq n_1, \\ &1 \leq t+2l' \leq n_2\} \end{aligned}$$

经过划分, 阵列 κ_{11} 内的元素发生改变与否相互间没有影响。因此, 阵列内元素的最优隐写转化为一般的加性失真最小问题, 这可以借助 STC 编码来解决。待该阵列内所有元素完成更新并嵌入信息后再处理 κ_{12} 中的元素, 依此类推即可实现一次完整的 Gibbs 扫描。

定义 2^[12] 如果子集 $c (c \subseteq \kappa)$ 内任意两个元素都构成相邻关系, 称 c 为一个基团 (clique)。

高阶邻域系统中较大的元素基团包含其内部小基团的全部关联信息, 因此, 失真定义时没有必要使用全部的元素基团, 只利用邻域系统内各个方向最大的基团参与失真定义, 这部分基团构成的集合记为 C , 如图 1 所示。

图像水平方向基团内两元素 x_i, x_j 间的关系为

$$D_{i,j}^{\rightarrow}(x) = x_i - x_j \quad (4)$$

$$i = 1, 2, \dots, n_1 n_2, j = 1, 2, \dots, n_1 n_2$$

嵌入信息后, 载体变为 y , $D_{i,j}^{\rightarrow}$ 的变化反映了嵌入操作给载体水平方向带来的影响, 即

$$H_{c \in C^{\rightarrow}}(y) = \sum_{x_i, x_j \in c, c \in C^{\rightarrow}} |D_{i,j}^{\rightarrow}(y) - D_{i,j}^{\rightarrow}(x)| \quad (5)$$

对垂直和对角方向的基团作相同的处理, 得到

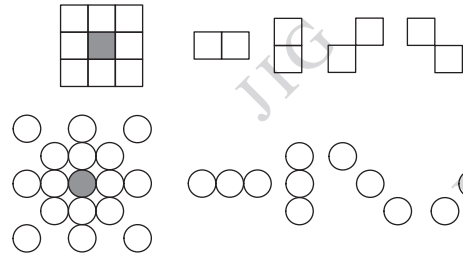


图 1 二阶、三阶邻域系统及本文所用元素基团

Fig. 1 Second-order neighborhood, third-order neighborhood and element cliques used in this paper

$H_{c \in C^{\uparrow}}(y), H_{c \in C^{\nearrow}}(y), H_{c \in C^{\nwarrow}}(y)$ 。 $H_c(y)$ 能够反映元素基团是否发生了修改及修改的幅度, 修改幅度越大 $H_c(y)$ 越大。在此基础上, 引入权重 ω 定义失真函数

$$D(y) = \sum_{c \in C} \omega H_c(y) \quad (6)$$

$$C = C^{\rightarrow} \cup C^{\nearrow} \cup C^{\uparrow} \cup C^{\nwarrow}$$

当 $c \in C^{\rightarrow}$ 时, $\omega = \left(1 + \theta \left| \sqrt{\sum_{x_i, x_j \in c} (D_{i,j}^{\rightarrow})^2} \right| \right)^{-1}$, 其他情况类似。这样设置权重会使嵌入修改更多地发生在纹理复杂区域。

根据式 (6) 可以得到元素 x_i 的局部失真表达

$$\rho_i(y'_i y_{-i}) = \sum_{c \in C, y_i \in c} \omega H_c(y'_i y_{-i}) \quad (7)$$

具体应用时, 可以将参数 θ 进一步细化, 使其对应不同的元素差分有不同的取值。由于图像的相关性, $D_{i,j}$ 取值的分布主要集中在 0 附近且两侧下降非常快, 故可以限定 $D_{i,j}$ 的范围, 令 $-T \leq D_{i,j} \leq T$ 。此时失真参数是一个向量 $\theta = (\theta_{-T}, \theta_{-T+1}, \dots, \theta_{T-1}, \theta_T)$, 相应的权重 $\omega = \left(1 + \sqrt{\sum_{x_i, x_j \in c} \theta(D_{i,j}^{\rightarrow})^2} \right)^{-1}$ 。

3 失真参数的优化

集成分类器^[13] 通过组合多个基本分类器的分类结果决定最终的分类, 降低了基本分类器分类假设的错误风险, 该方法的提出使隐写分析特征向高维发展, 出现了 SRM^[14]、PSRM^[15] 等隐写分析方法, 提高了隐写分析的准确率。与隐写分析类似, 隐写算法选择某种模型描述图像并在嵌入时保持该模型不变也面临着一定的风险。借助 Gibbs 抽样并多次优化失真参数 θ , 可以使算法集成多种特征子集, 避免对某一模型过度优化, 从而增强载密体的抗检测性。

构成集成分类器的基本分类器有很多, 目前普遍采用的是 Fisher 线性分类器。因此, 为了使隐写算法具有较强的抗检测性, 针对 Fisher 分类器探讨优化失真参数 θ 的标准。

3.1 参数优化标准

设样本数据阵 $U \in \mathbf{R}^{m \times N}$, 其中类型 I 有 N_1 个样本, 类型 II 有 N_2 个样本, $N_1 + N_2 = N$ 。两个类型的训练样本分别构成子集 U_1 和 U_2 。Fisher 判别法的基本思想是将两类 m 维数据投影到一条直线上, 使类与类之间尽可能分开。 m 维向量 u_j 通过投影变换 δ ($\delta \in \mathbf{R}^m$) 得到标量 v_j , 即 $v_j = \delta^T u_j, u_j \in U$ 。分类器的准则函数为

$$J_F(\delta) = \frac{|m_1 - m_2|^2}{s_1^2 + s_2^2} \quad (8)$$

式中, $m_i = \frac{1}{N} \sum_{v_j \in V_i} v_j, i=1, 2$, 表示映射到 1 维空间后的样本均值。 $s_i^2 = \sum_{v_j \in V_i} (v_j - m_i)^2, i=1, 2$, 表示映射后各类样本的类内离散度。

显然, 两类样本平均值之间的距离越大, 各类样本的类内离散度越小时, 分类效果越好, 即 J_F 越大分类效果越好。变换 J_F 使其成为 δ 的显函数, 利用 Lagrange 乘子法可得其极大值点^[16]

$$\delta^* = (S_\delta)^{-1} (M_1 - M_2) \quad (9)$$

式中, $M_i = \frac{1}{N} \sum_{u_j \in U_i} u_j, i=1, 2$, 表示样本均值向量。

$S_\delta = \sum_{i=1}^2 \sum_{u_j \in U_i} (u_j - M_i)(u_j - M_i)^T$ 为类内总离散度。

定理 1 对于确定的样本数据阵, Fisher 准则函数可取得的极大值为

$$J_{Fmax} = \frac{(M_1 - M_2)^T \left(\sum_{i=1}^2 \sum_{u_j \in U_i} (u_j - M_i)(u_j - M_i)^T \right)^{-1} (M_1 - M_2)}{(M_1 - M_2)^T (M_1 - M_2)} \quad (10)$$

证明 将 $m_i = \frac{1}{N} \sum_{v_j \in V_i} v_j, v_j = \delta^T u_j$ 和 $M_i =$

$\frac{1}{N} \sum_{u_j \in U_i} u_j$ 代入 $|m_1 - m_2|$ 和 $s_1^2 + s_2^2$ 中得

$$\begin{aligned} |m_1 - m_2| &= \left| \frac{1}{N_1} \sum_{v_j \in V_1} v_j - \frac{1}{N_2} \sum_{v_j \in V_2} v_j \right| = \\ &= \left| \frac{1}{N_1} \sum_{u_j \in U_1} \delta^T u_j - \frac{1}{N_2} \sum_{u_j \in U_2} \delta^T u_j \right| = \\ &= \left| \delta^T \left(\frac{1}{N_1} \sum_{u_j \in U_1} u_j - \frac{1}{N_2} \sum_{u_j \in U_2} u_j \right) \right| = \end{aligned}$$

$$\begin{aligned} &= |\delta^T (M_1 - M_2)| \\ s_1^2 + s_2^2 &= \sum_{i=1}^2 \sum_{v_j \in V_i} (v_j - m_i)^2 = \\ &= \sum_{i=1}^2 \sum_{u_j \in U_i} \left(\delta^T u_j - \frac{1}{N_i} \sum_{u_j \in U_i} \delta^T u_j \right)^2 = \\ &= \sum_{i=1}^2 \sum_{u_j \in U_i} \left(\delta^T (u_j - M_i) \right)^2 = \\ &= \sum_{i=1}^2 \sum_{u_j \in U_i} \delta^T (u_j - M_i) (u_j - M_i)^T \delta = \\ &= \delta^T S_\delta \delta \end{aligned}$$

当 $\delta = \delta^*$ 时, $J_F(\delta)$ 取得极大值

$$\begin{aligned} J_{Fmax} = J_F(\delta^*) &= \frac{|(\delta^*)^T (M_1 - M_2)|^2}{(\delta^*)^T S_\delta \delta^*} = \\ &= \frac{(\delta^*)^T (M_1 - M_2) \cdot (M_1 - M_2)^T \delta^*}{(\delta^*)^T S_\delta (\delta^*)^{-1} (M_1 - M_2)} = \\ &= \frac{(\delta^*)^T (M_1 - M_2) \cdot (M_1 - M_2)^T \delta^*}{(\delta^*)^T (M_1 - M_2)} = \end{aligned}$$

$$(M_1 - M_2)^T \delta^* = (M_1 - M_2)^T (S_\delta)^{-1} (M_1 - M_2)$$

所以有

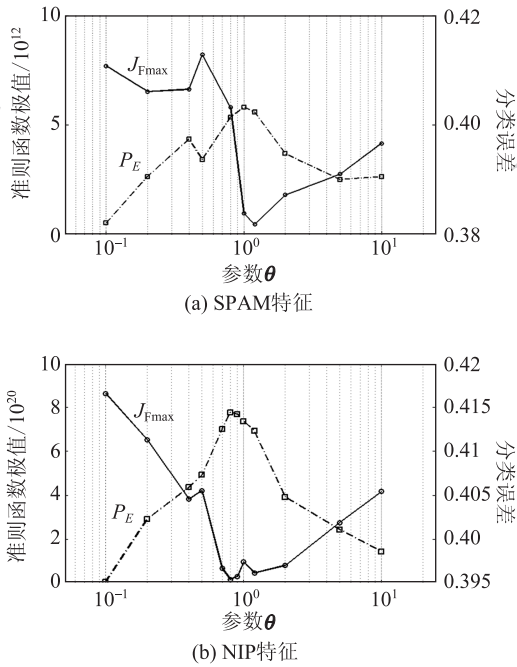
$$\begin{aligned} J_{Fmax} &= \\ &= (M_1 - M_2)^T \left(\sum_{i=1}^2 \sum_{u_j \in U_i} (u_j - M_i)(u_j - M_i)^T \right)^{-1} \times \\ &\quad (M_1 - M_2) \end{aligned}$$

证毕。

根据 θ 确定的失真函数设计最小失真隐写算法, 若所得 J_{Fmax} 越小说明 Fisher 线性分类器的分类效果越差, 隐写越安全。为了验证这一相关性, 进行以下实验:

令 θ 的维数为 1, 在四阶邻域系统下取 θ 不同的值得到相应的失真函数, 利用 STC 编码嵌入 0.5 bit/像素的随机信息。从中提取 100 幅载密图像及其原始载体的二阶 SPAM 特征^[17] 和 NIP 特征^[18] 计算得到 J_{Fmax} , 利用训练好的集成分类器检测这些图像得分类误差 P_E ($P_E = \min_{P_{FA}} \frac{1}{2} (P_{FA} + P_{MD}(P_{FA}))$)。实验结果如图 2 所示。

由图 2 可知, J_{Fmax} 的变化趋势与分类误差 P_E 的变化大体相反, 极值基本对应。又因为 J_{Fmax} 的取值可由定理 1 直接求得, 不需要大量图像以训练分类器, 计算开销小。所以, 虽然理论上 P_E 更能反映样本集的抗检测性, 本文选择 J_{Fmax} 作为参数 θ 的优化标准。

图2 不同特征集下 J_{Fmax} 和 P_E 随 θ 的变化情况Fig. 2 Change of J_{Fmax} and P_E with θ using different feature sets

3.2 特征子集的集成

基于 Gibbs 随机场的隐写以元素阵列为基本单元嵌入信息。因此,可以令不同的阵列对应不同的特征子集,进而对应不同的失真参数,从而实现隐写算法对多种特征子集的集成。

最优隐写下,向阵列 κ_{st} 中嵌入信息时,各元素以式(2)所得概率发生改变,式中 λ_{st} 由局部失真集 $\{\rho_i(y'_i y_{-i}) \mid i \in \kappa_{st}\}$ 确定。由于各阵列覆盖图像的不同区域且 θ 会因特征子集的不同有所差异, λ_{st} 可能随阵列的变化而变化,这与原本的 Gibbs 抽样有一定的偏差。不过,图像具有相关性,所以元素阵列间差别并不大。另一方面,通过合理控制特征子集的差异程度可以保证各阵列内元素失真构成的集合基本相同。因此, λ_{st} 会随着扫描次数的增加收敛于一个相同的值,整个过程依旧呈现 Gibbs 抽样的形式。

3.3 特征子集的构造

用于隐写分析的特征多种多样,多数这些特征 $F_i (i = 1, 2, \dots, d)$ 都可以写成局部统计量之和的形式, $F_i(x) = \sum_{c \in C} F_c^{(i)}(x)$ 。载体与载密体全部统计特征间的差别为^[4]

$$\|F(x) - F(y)\| = \sum_{i=1}^d \gamma_i |F_i(x) - F_i(y)| \leq$$

$$\sum_{i=1}^d \gamma_i \sum_{c \in C} |F_c^{(i)}(x) - F_c^{(i)}(y)| = \sum_{c \in C} \sum_{i=1}^d \gamma_i |F_c^{(i)}(x) - F_c^{(i)}(y)| \quad (11)$$

模型保持隐写就是将上式限制在较小的范围内从而使隐写分析无所作为,相应地,分析方可以选择其他特征参与检测以提高检测率。双方的对抗过程符合二人零和博弈问题。因此,借助博弈模型讨论特征子集的构造策略。

3.3.1 博弈模型的建立

设特征全集为 Z^n 。隐写方的策略是从 Z^n 中选择 m_a 维的特征并保持其隐写前后不变。相对地,分析方的策略是从中选择 m_b 个特征用于检测。固定 m_a, m_b 的大小,双方的策略集可以分别记为 $A = \{A_1, A_2, \dots, A_{C_n^{m_a}}\}$, $B = \{B_1, B_2, \dots, B_{C_n^{m_b}}\}$ 。博弈模型表示为

$$G = (A, B, Q) \quad (12)$$

式中, Q 为隐写方的支付矩阵,大小为 $C_n^{m_a} \times C_n^{m_b}$, Q 中元素 q_{ij} 表示博弈局势 (A_i, B_j) 下分析方的检测率。

定义3 两个特征子集 A_i, B_j 中相同元素的个数称为两集合的关联度 k , $k = g(A_i, B_j) = |A_i \cap B_j|$ 。

虽然隐写分析中各个特征对特定隐写算法检测成功的贡献不尽相同,但从整体上看,具体特征对一般隐写算法的检测影响可以忽略,即认为 $\gamma_1 = \gamma_2 = \dots = \gamma_d$ 。进一步地,可以认为 q_{ij} 的取值仅与 B_j 的有效特征数有关。故有

$$q_{ij} = f(m_b - k) = f(m_b - g(A_i, B_j)) \quad (13)$$

函数 f 是一个取值空间为 $[0.5, 1]$ 的单调递增函数。

3.3.2 模型的均衡分析

定理2 博弈模型下,隐写方的最佳策略为混合策略 $(\frac{1}{C_n^{m_a}}, \frac{1}{C_n^{m_a}}, \dots, \frac{1}{C_n^{m_a}})$ 。

证明 任意一方固定选择某策略时,对方都可以调整自身策略改变双方关联度 k 进而实现自身收益的最大化。因此,不存在纯策略纳什均衡,那么一定存在混合策略下的均衡局势^[19]。

设隐写方的混合策略为 $(a_1, a_2, \dots, a_{C_n^{m_a}})$, 则分析方在纯策略 B_j 下的期望收益为

$$\sum_{i=1}^{C_n^{m_a}} a_i Q_{ij} = \sum_{i=1}^{C_n^{m_a}} a_i f(m_b - g(A_i, B_j))$$

如果 $(a_1, a_2, \dots, a_{C_n^{m_a}})$ 是隐写方的最优策略,那

一定意味着分析方各个纯策略间是无差异的, 即

$$\sum_{i=1}^{C_n^{m_a}} a_i f(g(A_i, B_1)) =$$

$$\sum_{i=1}^{C_n^{m_a}} a_i f(g(A_i, B_2)) = \cdots = \sum_{i=1}^{C_n^{m_a}} a_i f(g(A_i, B_{C_n^{m_b}}))$$

此方程组的解为 $a_1 = a_2 = \cdots = a_{C_n^{m_a}}$ 。

又 $\sum_{i=1}^{C_n^{m_a}} a_i = 1$, 故此均衡局势下隐写方的混合策略

为 $(a_1, a_2, \cdots, a_{C_n^{m_a}}) = \left(\frac{1}{C_n^{m_a}}, \frac{1}{C_n^{m_a}}, \cdots, \frac{1}{C_n^{m_a}}\right)$ 。同理

可得分析方的混合策略 $(b_1, b_2, \cdots, b_{C_n^{m_b}}) = \left(\frac{1}{C_n^{m_b}}, \frac{1}{C_n^{m_b}}, \cdots, \frac{1}{C_n^{m_b}}\right)$ 。

证毕。

为了保证 λ_y 的收敛性, 特征子集构造时需要合理控制子集的差异程度, 所以各子集中大部分特征是相同的。在此前提下, 根据定理 2, 各子集中不同的部分应从全集中随机抽取产生。

定理 3 均衡局势下, 隐写方的期望支付仅与特征集的维数 m_a, m_b 有关, 期望支付为

$$E = \sum_{k=0}^m \frac{C_{m_a}^k \cdot C_{n-m_a}^{m_b-k}}{C_n^{m_b}} f(m-k) \quad (14)$$

$$m = \min(m_a, m_b)$$

证明 根据定理 2, 均衡局势下分析方选择各个策略的概率相等。因此, 对于隐写方任意的决策 A_i , 关联度 $g(A_i, B_j) = k$ 的概率仅与 m_a 和 m_b 的大小有关, 记为 $p(k, m_a, m_b)$ 。由组合数学理论可得

$$p(k, m_a, m_b) = \frac{C_{m_a}^k C_{n-m_a}^{m_b-k}}{C_n^{m_b}}$$

$$k = (0, 1, \cdots, \min(m_a, m_b))$$

因此, 在该博弈模型的均衡局势下, 隐写方的期望支付为

$$E = E(A, B) = \sum_{i=1}^{C_n^{m_a}} \sum_{j=1}^{C_n^{m_b}} a_i b_j q_{ij} =$$

$$\sum_{k=0}^m p(k, m_a, m_b) f(m_b - k) =$$

$$\sum_{k=0}^m \frac{C_{m_a}^k C_{n-m_a}^{m_b-k}}{C_n^{m_b}} f(m_b - k), m = \min(m_a, m_b)$$

证毕。

由定理 3 可知, 特征子集维数 m_a 的增大有助于降低隐写方的期望支付。在此基础上, 分别在 ITF 特征(120D)^[20]、NIP 特征(616D)、从 SRM 中抽取

的 2 000 维特征集下进行参数优化, 所得结果如图 3 所示。从图 3 中不难看出, 维数达到 2 000 时 P_E 随参数变化的趋势已不明显。这说明, θ 在特征维数增多时对失真函数优化的效果会减弱。综合以上结论, 实际应用时应应对 m_a 进行限定, 保证算法有良好的模型保持效果。

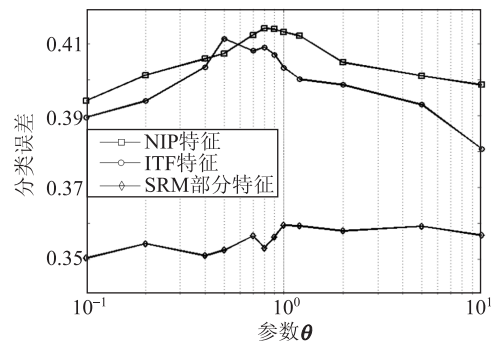


图 3 P_E 在不同维数特征集下随 θ 的变化情况

Fig. 3 Change of P_E with θ using feature sets of different dimensions

4 基于 Gibbs 随机场的隐写算法

4.1 算法流程

以 SPAM 特征、NIP 特征和 ITF 特征的合集作为特征全集 Z^n , 以检测效果较好的 SPAM 特征作为各子集的固定部分。若秘密信息比特数为 m , 本文隐写算法的具体流程表述如下:

1) 根据所采用的邻域系统将图像载体元素划分为 κ 个阵列, 初始化 $r = 1$;

2) 从特征全集 Z^n 中随机选择 $m_a - 686$ 个特征与 SPAM 特征共同构成特征子集, 针对该集合, 依据分类器极值 J_{Fmax} 对参数进行优化, 选择令 J_{Fmax} 取得极小值的参数 θ_r ;

3) 根据式(7)和 θ_r 计算修改元素 x_i 的局部失真代价 $y_i \rightarrow y'_i \in I_i$;

4) 利用双层 STC 编码向阵列 κ_r 中嵌入 $\frac{m}{R}$ 比特的信息并保证 $\sum_{i \in S_r} \rho_i(y'_i | y_{-i})$ 最小, 更新阵列 κ_r 中的元素;

5) 若 $r < \kappa$, 更新 $r = r + 1$, 返回第 2) 步, 否则转到下一步;

6) 重复以上 Gibbs 扫描和嵌入操作若干次, 所得载体密 y 将趋向于最优分布 φ_λ 的样本。

对于接收方,如果保证收发双方采用相同的邻域系统,那么,只需知道秘密信息的长度就可以通过双层 STC 编码正确提取出信息。

4.2 实验结果与分析

图4—图6给出了文献[4]算法、文献[8]算法和本文算法在不同的隐写分析特征集下的分类误差。图4—图6中所示结果为10次检测的平均值,实验中保证本文算法各次构造的特征子集相同。实验所用1200幅图像全部来自NRCS图像库,实验前将其全部转换并裁剪为 512×512 像素的png灰度图。实验采用集成分类器作为分类检测工具。实验中3种算法的元素修改方式均为 ± 1 修改,文献[4]和本文算法均采用四阶邻域系统,本文算法限定特征子集规模为1000维, θ 的维数为1,Gibbs抽样的扫描次数为3,STC编码的子矩阵高 $h=10$ 。

根据图4可知,与同样针对SPAM特征设计的文献[8]算法相比,本文算法能更好地抵抗SPAM检测。由图5、图6可以看出,该算法没有出现过度优化的情况,在扩展后的特征全集下依然具有相当的抗统计分析能力,即使在高维特征集下的安全性

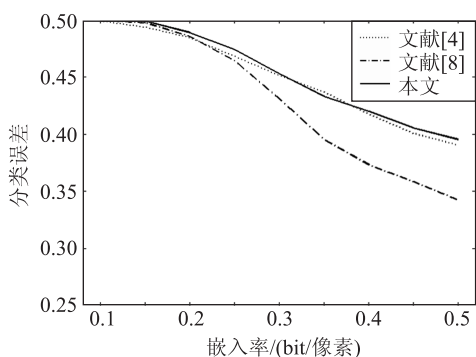


图4 SPAM特征检测结果(686维)

Fig. 4 Experimental results using the SPAM set

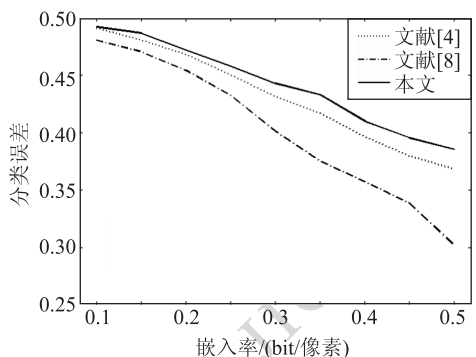


图5 特征全集 Z^n 检测结果(1422维)

Fig. 5 Experimental results using the ensemble set Z^n

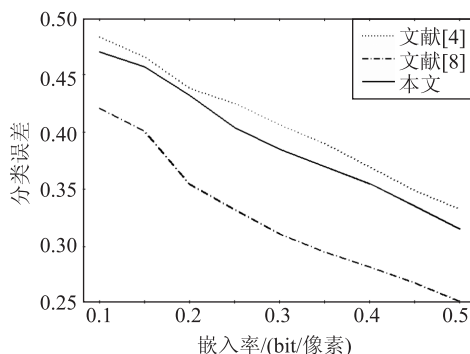


图6 SRM特征检测结果(3467维)

Fig. 6 Experimental results using the SRM set

也较好。观察图4还发现,文献[4]的算法虽然不属于模型保持隐写,但在SPAM特征下的抗检测性也很好,这是因为其失真函数的设计以共生矩阵为基础,与SPAM特征构造相吻合。另外,值得说明的是,通过增大 θ 的维数,本文算法还可以进一步提高模型保持的能力。

5 结论

抗统计分析的隐写算法设计是目前隐写研究的核心,但是,无论是最小失真隐写还是模型保持隐写都有各自明显的弊端。针对这一现状,本文提出了一种最小化嵌入失真隐写算法,利用Gibbs随机场理论集成多个有所区别的特征子集实现信息的嵌入。本文算法是模型保持的通用算法,能用于保持任意特征集,而且能够应用于JPEG图像。实验结果表明,该算法具有较好的适应性和安全性,能够在保持特定特征集的基础上有效避免对模型的过度优化。接下来的工作是进一步挖掘元素改变相互间影响,设计更为合理的失真函数,提高载密体抵抗高维统计分析的能力。

参考文献 (References)

- [1] Filler T, Judas J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935. [DOI: 10.1109/TIFS.2011.2134094]
- [2] Kim Y, Duric Z, Richards D. Modified matrix encoding technique for minimal distortion steganography[C] // Proceedings of the 8th Information Hiding International Workshop. Berlin: Springer-Verlag, 2006: 314-327. [DOI: 10.1007/978-3-540-74124-4_21]

- [3] Sachnev V, Kim H J, Zhang R. Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding[C] // Proceedings of the 11th ACM Multimedia & Security Workshop. New York: ACM Press, 2009: 131-140. [DOI: 10. 1145/1597817. 1597841]
- [4] Filler T, Fridrich J. Gibbs construction in steganography[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 705-720. [DOI: 10. 1109/TIFS. 2010. 2077629]
- [5] Agaian S S, Sifuentes R R. Adaptive steganography with increased embedding capacity for new generation of steganographic systems[C] // Proceedings of Image Processing: Algorithms and Systems IV. Bellingham: SPIE Press, 2005, 5672: 257-268. [DOI: 10. 1117/12. 588032]
- [6] Lou D C, Wu N I, Wang C M, et al. A novel adaptive steganography based on local complexity and human vision sensitivity[J]. Journal of Systems and Software, 2010, 83(7): 1236-1248. [DOI: 10. 1016/j. jss. 2010. 001. 050]
- [7] Zhang Z, Liu G J, Dai Y W, et al. A self-adaptive image steganography algorithm based on cover-coding and markov model[J]. Journal of Computer Research and Development, 2012, 49(8): 1668-1675. [张湛, 刘光杰, 戴跃伟, 等. 基于隐写编码和 Markov 模型的自适应图像隐写算法 [J]. 计算机研究与发展, 2012, 49(8): 1668-1675.]
- [8] Filler T, Fridrich J. Design of adaptive steganographic schemes for digital images[C] // Proceedings of Media Watermarking, Security, and Forensics III. Bellingham: SPIE Press, 2011, 7880: 1-14. [DOI: 10. 1117/12. 872192]
- [9] Kodovsky J, Holub V. On dangers of overtraining steganography to incomplete cover model[C] // Proceedings of ACM Multimedia & Security Workshop. New York: ACM Press, 2011: 69-76. [DOI: 10. 1145/2037252. 2037266]
- [10] Kodovsky J, Fridrich J. On completeness of feature spaces in blind steganalysis[C] // Proceedings of the 10th ACM Multimedia & Security Workshop. New York: ACM Press, 2008: 123-132. [DOI: 10. 1145/1411328. 1411352]
- [11] Kodovsky J, Fridrich J. Steganalysis of JPEG images using rich models[C] // Proceedings of SPIE Media Watermarking, Security, and Forensics. Bellingham: SPIE Press, 2012, 8303: 1-13. [DOI: 10. 1117/12. 907495]
- [12] Li X C, Zhu S A. A survey of the markov random field method for image segmentation[J]. Journal of Image and Graphics, 2007, 12(5): 789-798. [李旭超, 朱善安. 图像分割中的马尔可夫随机场方法综述[J]. 中国图象图形学报, 2007, 12(5): 789-798.] [DOI: 10. 11834/jig. 20070504]
- [13] Kodovsky J, Fridrich J, Holub V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 432-444. [DOI: 10. 1109/TIFS. 2011. 2175919]
- [14] Fridrich J, Kodovsky J. Rich models for steganalysis of digital images[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 868-882. [DOI: 10. 1109/TIFS. 2012. 2190402]
- [15] Holub V, Fridrich J, Denemark T. Random projections of residuals as an alternative to co-occurrences in steganalysis[C] // Proceedings of Media Watermarking, Security, and Forensics. Bellingham: SPIE Press, 2013, 8665: 1-11. [DOI: 10. 1117/12. 1000330]
- [16] Chen C K, Yang J Y. Fisher large margin linear classifier[J]. Journal of Image and Graphics, 2007, 12(12): 2143-2147. [陈才扣, 杨静宇. Fisher 大间距线性分类器[J]. 中国图象图形学报, 2007, 12(12): 2143-2147.] [DOI: 10. 11834/jig. 20071218]
- [17] Pevny T, Bas P, Fridrich J. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 215-224. [DOI: 10. 1109/TIFS. 2010. 2045842]
- [18] Guan Q X, Dong J, Tan T N. An effective image steganalysis method based on neighborhood information of pixels[C] // Proceedings of 18th IEEE International Conference on Image Processing. Washington: IEEE Computer Society, 2011: 2721-2724. [DOI: 10. 1109/ICIP. 2011. 6116231]
- [19] Nash J. Equilibrium points in n-person games[J]. Proceedings of the National Academy of Sciences of the United States of America, 1950, 36: 48-49.
- [20] Xiong G, Ping X J, Zhang T, et al. Image textural features for steganalysis of spatial domain steganography[J]. Journal of Electronic Imaging, 2012, 21(3): 033015(1-15). [DOI: 10. 1117/1. JEL. 21. 3. 033015]