

基于多元回归的 JPEG 隐密分析方案

郭艳卿¹, 何德全¹, 孔祥维¹, 尤新刚^{1,2}

(1. 大连理工大学信息安全中心, 辽宁大连 116024; 2. 北京电子技术应用研究所, 北京 100091)

摘要: 为解决 JPEG 图像隐密分析算法的设计问题, 在 DCT 域共生矩阵的基础上构建了 JPEG 图像共生特征空间, 并将定量隐密分析算法看成多元共生特征与含密量之间的回归模型, 提出了一种 JPEG 图像定量隐密分析算法设计方案. 此方案以已知含密量的 JPEG 图像为研究对象, 而无需分析对应的 JPEG 隐密机制, 因此具有较强的通用性. 实验结果表明, 对安全性较高的 MBI 隐密算法, 本文方案仍可设计出高检测能力的定量隐密分析方法.

关键词: 多元回归; JPEG; 隐密分析; 共生特征; MBI

中图分类号: TP35 **文献标识码:** A **文章编号:** 0372-2112 (2009) 06-1378-04

Steganalytic Scheme for JPEG Images Based on Multivariate Regression

GUO Yarr qing¹, HE Der quan¹, KONG Xiangwei¹, YOU Xin gang^{1,2}

(1. Information Security Research Center, Dalian University of Technology, Liaoning, Dalian 116024, China;

2. Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

Abstract: A co-occurrence feature space is constructed, which can effectively reflect the changes of higher order statistical characteristics caused by JPEG steganographic techniques. Supported by this feature space, a new scheme for designing steganalytic algorithms is presented based on multivariate regression model. With only JPEG stego images and no embedding details needed, this designing scheme is able to provide a good generality. Experimental results indicate that, our designing scheme can also produce remarkable steganalytic algorithm even for MBI embedding mechanism, which has reached high performance of security.

Key words: multivariate regression; JPEG, steganalysis, co-occurrence feature, MB(model based)

1 引言

隐密分析(Steganalysis)是用于检测、分析甚至破译网络传输数据中所隐藏的秘密信息的技术^[1]. 通常所说的隐密分析大都是指被动隐密分析, 即在不修改待测数据的前提下进行, 可分为通用性隐密分析和定量隐密分析两类. 通用性隐密分析通过提取高维统计特征建立特征空间, 再利用已知样本所训练出的分类器对待测样本进行分类判决, 判断其是否含有秘密信息; 而针对特定隐密方法设计的定量分析方法不但可以判断待测样本是否含密, 而且还可以估计出待测样本内的秘密信息隐藏量.

由于定量隐密分析对后续的分析甚至破译工作都有着十分重要的实际意义, 因此受到了各国学者的广泛关注. 如张涛等人曾针对 JSteg 类隐密算法提出了一种快速、准确的定量隐密分析方法^[2], 用于估计待测图像中含有 JSteg 隐密信息的长度. 依据类似的概率推导思想, Fridrich 结合对原始载体 JPEG 图像的估计技术, 设

计了针对 F5、OutGuess 隐密算法的定量隐密分析方法^[3,4]. 然而, 对于具有更为复杂嵌入机制的隐密算法, 由于统计特征量与秘密信息隐藏量之间概率关系难以推导, 因此很难进行定量隐密分析. 如对于安全性较高的 MBI^[5]、PQ^[6]隐密算法, 目前仍只能进行准确性较低的判决性隐密分析而无法定量分析^[7,8].

针对 JPEG 图像的定量隐密分析问题, 本文利用 DCT 系数之间的相关性提取 DCT 域多元统计特征量, 以更为全面地反映复杂嵌入机制对 DCT 系数引入变化规律, 并采用多元回归技术拟合统计特征量与秘密信息隐藏量之间的关系, 提出了一种具有较强通用性的定量隐密分析方案.

2 JPEG 图像共生特征

存在与秘密信息隐藏量相关的统计特征量是隐密分析的前提条件, 而统计特征量的敏感性是影响定量隐密分析算法精度的主要因素. 目前, 已有的定量隐密分析算法大都采用单一统计特征量作为秘密信息隐藏量

的度量依据. 单一统计特征量所包含的信息毕竟有限, 且针对某种特定隐密算法提取的统计特征量往往很难用于分析其他隐密算法. 另一方面, 近年来国内外学者对通用性隐密分析算法的研究表明, 高维统计特征空间可更全面、更有效地反映各种 JPEG 隐密算法可能对图像数据造成的影响^[9, 10]. 因此, 本文借鉴共生矩阵的思想, 在 DCT 域共生矩阵的基础上提取 JPEG 图像的多元共生特征, 用于后续的隐密分析方案.

2.1 DCT 域共生矩阵

设一幅 JPEG 图像 8×8 块的量化后 DCT 系数矩阵为 $J_{r,c}(i,j)$, 其中 $1 \leq r \leq R, 1 \leq c \leq C$ 分别表示此图像 8×8 块的行列序号, $1 \leq i, j \leq 8$ 分别表示在 8×8 块中量化后 DCT 系数的行列序号.

则, JPEG 图像 DCT 域共生矩阵 F_J 定义为:

$$F_J(p_1, p_2) = \frac{1}{2} \sum_{r=1}^{R-1} \sum_{c=1}^{C-1} \sum_{i,j=1}^8 \prod_{k=1}^2 [\delta(J_{r+c-k-1,c}(i,j) - p_k) + \delta(J_{r,c+k-1}(i,j) - p_k)] \quad (1)$$

其中, $\delta(x) = \begin{cases} 1, & x = 0 \\ 0, & x \neq 0 \end{cases}, p_1, p_2 \in \{-T, -T+1, \dots, T\}$ 为量化后 DCT 系数值, T 为正整数参数.

2.2 JPEG 图像共生特征

由于图像内容的差异, 不同载体 JPEG 图像的 DCT 域共生矩阵会存在一定差别, 致使隐藏相同长度秘密信息后含密图像的 DCT 域共生矩阵值存在一定波动. 为尽可能消除此偏差、更好地突出隐密操作造成的统计特征变化, 本文采用文献[3, 4]中的剪切—重压缩操作对统计特征进行校准.

设待测 JPEG 图像 J 的 8×8 块量化后 DCT 系数矩阵为 $J_{r,c}(i,j)$, 其剪切 4 行 4 列重新压缩后的校准 JPEG 图像系数矩阵为 $J'_{r,c}(i,j)$. 其中 $1 \leq r \leq R, 1 \leq c \leq C$ 分别表示此图像 8×8 块的行列序号, $1 \leq i, j \leq 8$ 分别表示在 8×8 块中量化后 DCT 系数的行列序号.

则 JPEG 图像的共生特征 V_J 定义为 DCT 域共生矩阵的相对变化量, 表达式为:

$$V_J = \frac{F_J(p_1, p_2) - F'_J(p_1, p_2)}{F_J(p_1, p_2)} \quad (2)$$

例如, 一幅 JPEG 图像 $J_{r,c}$ 和校准图像 $J'_{r,c}$ 的 DCT 域共生矩阵分别如表 1 和表 2 所示.

表 1

$F_{J,2}(p_1, p_2)$	$p_1 = -1$	$p_1 = 0$	$p_1 = 1$
$p_2 = -1$	52712	130316	50473
$p_2 = 0$	131078	1621981	130351
$p_2 = 1$	50602	128731	51960

则 $J_{r,c}(i,j)$ 的共生特征为:

$$V_{J,2} = \frac{F_J(p_1, p_2) - F'_J(p_1, p_2)}{F_J(p_1, p_2)} = \begin{bmatrix} -0.0905 & -0.0504 & -0.0927 \\ -0.0472 & 0.0395 & -0.0337 \\ -0.0953 & -0.0359 & -0.0697 \end{bmatrix}$$

表 2

$F_{J,2}(p_1, p_2)$	$p_1 = -1$	$p_1 = 0$	$p_1 = 1$
$p_2 = -1$	57959	137228	55628
$p_2 = 0$	137573	1560283	134895
$p_2 = 1$	55930	133527	55853

3 基于多元回归的隐密分析方案

定量隐密分析的本质是寻找统计特征量与秘密信息隐藏量之间的函数关系, 以建立可用于预测待测数据中秘密信息隐藏量的定量隐密分析模型. 对于某一特定隐密算法, 可以依据大量的统计实验数据建立定量分析模型. 在此假设可获取的 k 个图像数据统计特征 $x_1, x_2, \dots, x_k$ 与秘密信息隐藏量 y 之间存在一定的可预测关系, 本文将对此关系建立回归模型进行拟合, 并通过显著性检验验证模型的拟合精度, 完成定量隐密分析算法的设计.

3.1 隐密分析算法的基本原理

由于具有不同嵌入机制的隐密算法所产生的可预测可能存在较大差异, 为适合对复杂隐密算法进行定量分析, 我们采用二次非线性回归模型拟合多元统计特征量和秘密信息隐藏量. 设 n 幅已知秘密信息隐藏量的含密图像所对应的观测值为 $(x_{i1}, x_{i2}, \dots, x_{ik}, y_i)$, 则建立如下的回归模型^[11]:

$$y_i = \sum_{j=1}^k (\beta_j x_{ij} + \beta_{j+1} x_{ij}^2) + \varepsilon_i, i = 1, 2, \dots, n \quad (3)$$

其中 $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ 是不可观测的随机误差, 通常称为试验误差.

令

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}, \quad X = \begin{bmatrix} x_{11}x_{12} \dots x_{1k}x_{11}^2x_{12}^2 \dots x_{1k}^2 \\ x_{21}x_{22} \dots x_{2k}x_{21}^2x_{22}^2 \dots x_{2k}^2 \\ \vdots \\ x_{n1}x_{n2} \dots x_{nk}x_{n1}^2x_{n2}^2 \dots x_{nk}^2 \end{bmatrix},$$

$$B = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{2k} \end{bmatrix}, \quad \xi = \begin{bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{bmatrix},$$

则式(3)的简化形式为:

$$Y = XB + \xi \quad (4)$$

其中 B 为待估计的未知参数, 称为回归系数. 在数理统计学中, 此多元线性回归模型可应用最小二乘法求得 B 的无偏估计量 $\hat{B}$.

$$\hat{B} = (X' \cdot X)^{-1} \cdot X' \cdot Y \quad (5)$$

则可得如下某一特定隐密算法的定量隐密分析式:

$$\hat{Y} = XB \tag{6}$$

这样, 如果可以计算出待测 JPEG 图像 $J_{r,c}$ 的 k 个统计特征值 $x_1, x_2, \dots, x_k$, 则 $J_{r,c}$ 内秘密信息隐藏量的预测值为:

$$\hat{y} = \sum_{j=1}^k (\hat{\beta}_{x_j} + \hat{\beta}_{x_j} x_j^2) \tag{7}$$

3.2 隐密分析模型的显著性检验

模型检验是定量隐密分析模型的一个重要部分, 其结果好坏直接决定了模型的预测能力和真实有效性. 本文采用数理统计中的相关系数检验法^[11]来度量所得模型与真实函数关系之间的拟合程度. 其基本原理为:

考虑恒等式 $y_i - \hat{y}_i = (y_i - \bar{y}) - (\hat{y}_i - \bar{y})$, 其中 $\bar{y} = E(y)$ 为 y 的均值. 该式意味着将残差 $e_i = y_i - \hat{y}_i$ 分成两个量之差: 观察值 y_i 离均值 $\bar{y}$ 的偏差和估计值 $\hat{y}_i$ 离 $\bar{y}$ 的偏差.

令 $R_1^2 = \frac{SS_r}{SS_t} = \frac{\sum_{i=1}^n (\hat{y}_i - \bar{y})^2}{\sum_{i=1}^n (y_i - \bar{y})^2}$, 称 R_1^2 为测定系数.

显然 $R_1^2 \leq 1$. R_1^2 越接近 1, 则说明引起因变量 y 的变异性更多的是通过关于自变量 x 的回归来解释, 即线性回归模型与样本观察值拟合优度越好; R_1^2 接近于 0 说明引起 y 的变异性极少是通过关于 x 的回归来解释, 即线性回归方程与样本观察值拟合的不理想; $R_1^2 = 1$,

说明引起 y 的变异性可完全由关于 x 的回归来解释.

4 实验结果与讨论

为验证本文所提共生特征和隐密分析算法设计方案的有效性, 我们以针对 MBI^[5] 设计的定量隐密分析算法为例, 使用了大量图像样本与文献[7]的方法进行了多批量比较测试. 实验中载体 JPEG 图像样本是由 1300 幅高精度数码相机图像(来源于 50 种不同型号的数码相机)经 ACDSec7.0 缩放、重压缩得到(质量因数为 85), 其中 800 幅用于生成训练样本, 500 幅用于生成测试样本. 含密图像样本由上述载体 JPEG 图像样本经 MBI 隐密算法生成, 秘密信息隐藏量分别为 10%, 20%, ..., 100%, 即共有 8800 幅训练样本, 5500 幅测试样本.

实验中我们选取参数 $T = 2$, 提取 8800 幅训练样本集中每幅 JPEG 图像的 50 维共生特征, 组成 8800 行 50 列统计特征观测矩阵 X , 再由每幅 JPEG 图像的秘密信息隐藏量组成 8800 行 1 列的观测矩阵 Y , 其中 $y_i \in \{0, 0.1, 0.2, \dots, 1\}$. 根据式(3)~(7)求得二次非线性回归模型参数 $\hat{B}$, 如表 3 所示. ($\hat{B}$ 一次 $\hat{B}$ 二次分别代表一次和二次参数)

在表 3 参数下, 计算得测定系数 $R_1^2 = 0.9512$, 说明此二次非线性回归模型与样本观察值具有较好的拟合优度, 此参数下针对 MBI 的定量隐密分析算法具有较强的检测能力.

表 3 针对 MBI 的定量隐密分析算法参数 $\hat{B}$

P_1, P_2	$\hat{B}$ 一次	$\hat{B}$ 二次	P_1, P_2	$\hat{B}$ 一次	$\hat{B}$ 二次	P_1, P_2	$\hat{B}$ 一次	$\hat{B}$ 二次	P_1, P_2	$\hat{B}$ 一次	$\hat{B}$ 二次	P_1, P_2	$\hat{B}$ 一次	$\hat{B}$ 二次
-2, -2	-0.2998	-0.0420	-1, -2	0.3145	2.5923	0, -2	0.7701	-0.8389	1, -2	-0.1861	-0.7254	2, -2	-0.6692	-1.6568
-2, -1	-0.2939	1.3477	-1, -1	1.1027	4.6251	0, -1	1.8914	10.8248	1, -1	0.5970	-0.4879	2, -1	0.2632	4.7706
-2, 0	0.5214	-0.8817	-1, 0	-2.5572	-16.1873	0, 0	4.0218	-7.6599	1, 0	-1.1459	-10.3471	2, 0	0.4101	0.2016
-2, 1	-0.3272	0.1102	-1, 1	1.2075	1.2270	0, 1	0.0168	14.1849	1, 1	0.5749	0.3173	2, 1	-0.1805	2.8008
-2, 2	-0.1419	-0.3426	-1, 2	0.4914	1.6846	0, 2	1.0080	-0.2570	1, 2	0.1323	0.0131	2, 2	-0.3894	-0.6905

表 4 本文算法与文献[7]算法的实验结果比较

检测性能 虚警率	文献[7]算法在不同嵌入容量下的检测率						本文算法在不同嵌入容量下的检测率					
	10%	20%	40%	60%	80%	100%	10%	20%	40%	60%	80%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
90%	93.0%	96.6%	98.8%	100%	100%	100%	100%	100%	100%	100%	100%	100%
80%	85.0%	88.8%	97.2%	99.8%	100%	100%	100%	100%	100%	100%	100%	100%
70%	77.8%	84.6%	94.8%	99.8%	100%	100%	100%	100%	100%	100%	100%	100%
60%	65.4%	71.6%	89.4%	99.0%	100%	100%	99.8%	100%	100%	100%	100%	100%
50%	56.8%	63.4%	85.2%	98.6%	100%	100%	99.4%	100%	100%	100%	100%	100%
40%	47.4%	55.8%	79.8%	96.2%	100%	100%	99.4%	100%	100%	100%	100%	100%
30%	34.6%	47.4%	70.6%	92.8%	100%	99.8%	98.8%	100%	100%	100%	100%	100%
20%	25.8%	37.6%	60.4%	87.8%	99.8%	99.2%	96.4%	100%	100%	100%	100%	100%
10%	14.8%	21.4%	42.6%	72.2%	94.4%	95.4%	91.6%	100%	100%	100%	100%	100%
0%	0.2%	0.2%	1.4%	4.2%	14.6%	13.0%	3.8%	78.4%	100%	100%	100%	100%

为进一步验证本文算法的检测性能, 我们将表 3 参数确定的定量隐密分析算法同参考文献[7]隐密分析

算法进行了性能比较(本文算法仍采用表 3 中参数). 对比实验中的测试图像由 MBI 隐密算法生成的 10%,

20%, 40%, 60%, 80%, 100% 含密图像组成, 分别计算两种隐密分析算法在不同虚警率情况下对 5 批含密图像的检测率。

从表 4 中实验结果可以看出, 文献[7] 算法对较高含密度(大于 60%) 的 MB1 图像具有一定的检测能力, 当虚警率大于 10% 时检测率大于 72.2%, 但对低含密度(如 10%、20%) MB1 图像的虚警率和检测率近乎相等, 说明几乎无检测能力。而本文算法对 MB1 含密图像的检测性能远优于文献[7] 算法。当嵌入容量大于 40% 时, 本文算法在无虚警前提下达到 100% 的检测率。对 10% 嵌入容量的低含密度 MB1 图像, 当虚警率为 10% 时, 检测率仍可达 90% 以上。对比检测结果表明, 本文算法的检测性能远优于已有的检测算法, 可用于 MB1 隐密图像的有效检测。

5 结论与展望

本文针对 JPG 图像定量隐密分析面临的两个关键问题, 分别提出了 JPEG 图像共生特征提取方法和基于多元回归的隐密分析方案, 并将 JPG 图像定量隐密分析工作融入统一框架下, 提出了通用的定量隐密分析算法设计方案。针对 MB1 的定量隐密分析实验表明, 依据本文所提方案设计出的定量隐密分析方法可具有较强的检测能力。

由于剪切—重压缩的校准过程并不能完全估计出原始载体图像的统计特征, 因此本文用于定量隐密分析设计的高阶共生特征会在一定程度上受 JPEG 图像参数的影响(基于剪切—重压缩的其他 JPEG 图像定量隐密分析算法也存在同样的问题), 即用质量因数为 85 的 JPEG 图像估计出的模型参数在检测其他质量的 JPEG 图像时预测值会有少量偏差。对于此问题, 可事先由不同质量 JPEG 图像得出多个模型参数, 检测时根据待测 JPEG 图像的量化表选择最适合的模型参数进行定量隐密分析。

参考文献:

- [1] Fabien A P Petitcolas, Ross J Anderson, Markus G Kuhn. Information hiding a survey[J]. IEEE Special Issue on Protection of Multimedia Content, 1999, 87(7): 1062–1078.
- [2] Tao Zhang, Xijian Ping. A Fast and Effective Steganalytic Technique against Jsteg-Like Algorithms[A]. Proceedings of ACM Symposium on Applied Computing[C]. Florida USA: ACM Press, 2003. 307–311.
- [3] Fridrich J, Goljan M, Hoge D. Steganalysis of JPEG images: breaking the F5 algorithm[A]. Proceeding of 5th Information Hiding Workshop[C]. Noordwijkerhout Netherlands: Springer Verlag, 2002. 310–323.
- [4] Fridrich J, Goljan M, Hoge D. Attacking the OutGuess[A]. Proceedings of the ACM Workshop on Multimedia and Security 2002[C]. Juan les Pins France: ACM Press, 2002. 3–6.
- [5] Sallee P. Model based steganography[A]. Proceedings of International Workshop on Digital Watermarking[C]. Busan Korea: Springer Verlag, 2004. 154–167.
- [6] Fridrich J, Goljan M, Soukal D. Perturbed quantization steganography with wet paper codes[A]. Proceedings of ACM Multimedia Security Workshop[C]. Magdeburg Germany: ACM Press, 2004. 4–15.
- [7] Bohme R. Breaking Cauchy model based JPEG steganography with first order statistics[A]. Proceedings of 9th European Symposium on Research in Computer Security[C]. Sophia Antipolis France: Springer-Verlag, 2004. 125–140.
- [8] Gökhan Gül, Ahmet Emir Dirik, Ismail Avciabas. Steganalytic features for JPEG compression based perturbed quantization[J]. IEEE Signal Processing Letters. 2007, 14(3): 205–208.
- [9] Pevny T, Fridrich J. Merging Markov and DCT features for multi class JPEG steganalysis[A]. Proceedings of Security Steganography and Watermarking of Multimedia Contents IX[C]. San Jose USA: SPIE Press, 2007. 3–4.
- [10] Wang Y, Moulin P. Optimized feature extraction for learning based image steganalysis[J]. IEEE Trans. on Information Forensics and Security, 2007, 2(1): 31–45.
- [11] 藤素珍, 冯敬海. 数理统计学[M]. 大连: 大连理工大学出版社, 2005. 199–224.

作者简介:



郭艳卿 男, 1980 年出生于辽宁省新民市。2002 年毕业于大连理工大学电子工程系。现为大连理工大学博士研究生, 研究方向: 信息隐藏、信号与信息处理。

E-mail: sagat823@yahoo.com.cn



何德全 男, 1933 年出生于北京。1994 年当选为中国工程院院士, 信息技术专家, 国家信息化专家咨询委员会副主任。在信息防护与安全技术、新型显示与处理技术、信息光学与化学等多个领域, 有较高的学术造诣。取得了 20 余项高难度、高水平的科技成果, 其中 10 项获国家发明二等奖、国家科技进步奖及部级科技进步奖。

E-mail: hedq@dlut.edu.cn