图象信息隐藏检测研究①

Research of Steganalysis On Images

周继军 （北京邮电大学信息安全中心 100876）
王 颖 （北京 202 信箱 71 分箱 102600）
钮心忻 （北京邮电大学信息安全中心 100876）

摘要：图象信息隐藏检测研究已经成为学术界在网络与信息安全领域中一项重要的攻关课题。本文首先介绍了典型的图象信息隐藏检测算法并给出了算法评价，然后指出了当前图象信息隐藏检测的攻关难点和下一步的研究方向。

关键词：信息隐藏 检测

1 引言

美国 911 事件发生以后，信息隐藏技术被怀疑为恐怖分子采用的秘密通信手段之一，由此掀起了全世界信息隐藏检测的研究热潮。所谓图象信息隐藏就是将秘密信息隐藏在图象中通过因特网传输的隐蔽通信技术，国外学术界将其称为能保证信道和信源均安全的高级信息安全技术。一个通用的图象信息隐藏系统可以描述为：待隐藏的秘密信息（隐藏对象）在密钥（Key）的控制下，通过嵌入算法将隐藏对象隐藏于图象掩体中形成隐藏载体，隐藏载体通过信道（网络）传输，在终端利用密钥从隐藏载体中恢复出隐藏对象的过程。目前在因特网上已经发布了接近 300 种图象信息隐藏软件而且据统计每周都有一种新的软件或一个新的软件版本出现，这些软件具有较广的适用性，JPG、GIF、PNG、PCX、BMP、TIFF、TGA、AVI、MPEG 等图象都能作为隐藏信息的图象掩体。由于信息隐藏分析者只能截获可能的隐藏载体而对嵌入密钥、图象掩体、信息的隐藏位置、嵌入算法、信息加密密钥都是未知的，因此信息隐藏分析是一件十分困难的研究工作，但这正引起了众多科研工作者的兴趣，他们在许多学科领域中都建立了相应的隐藏检测算法。本文的目的就是要介绍、比较和分析这些检测算法，由此引出隐藏检测算法研究难点和未来的研究方向。

2 图象信息隐藏检测方法

2.1 视觉检测

视觉检测利用了人类视觉系统可以清晰分辨噪声和图像轮廓的能力。图象信息隐藏算法设计时往往假设图像中 LSB（Least Significant Bit）位是完全随机的，也就是看作噪声，可以被任意替换。但是以上假设只能相对于机器才有意义，其原因是由于现代科技还不能完成类似人眼那样具有高智能的计算机程序，因此连续的空域隐藏很容易受到视觉检测。一些流行的隐藏软件例如 courier、s－tools、securengine、wbStego、Steganos Security Suite、eShow 等对 BMP 图象隐藏中都能被视觉检测。图 1 给出了使用 securengine 软件隐藏秘密信息前后图象掩体 LSB 平面的变化。很显然图 1 右下方风“风车”隐写载体中下方的轮廓已经被嵌入信息覆盖了。

2.2 特征码检测

许多图象信息隐藏软件会在隐藏信息的同时将特定意义的标记（特征码），利用数字嵌入的方法隐藏在图象中，用以证明创作者对其作品的所有权，并作为鉴定、起诉非法侵权的证据，同时通过对特征码的检测和分析来保证数字信息的完整可靠性，从而成为知识产权保护和数字多媒体防伪的有效手段[1]。但是脆弱的软件防伪技术恰恰成为了信息隐藏检测的突破点，许

① 国家“973”项目资助（编号 G1999035804），教育部优秀青年教师资助项目，国家自然科学基金（60473016）

多检测方法就是通过大量比较隐藏前后图象掩体和图象隐藏载体的差异找到特征码从而对留有特征码的隐藏软件检测的成功率可高达 99.9% 以上。目前，因特网上所公布的图象隐藏软件大概有 20% 都能找到特征码。

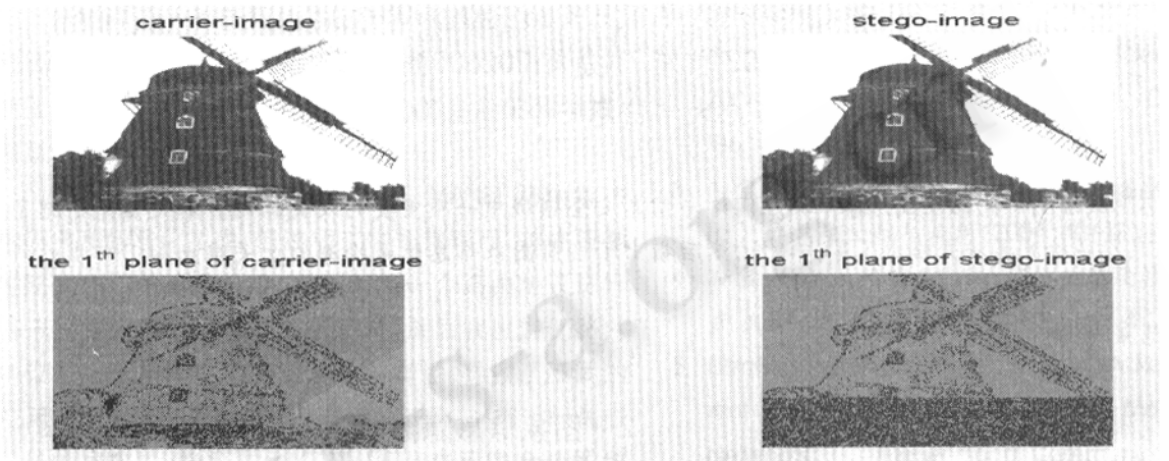

图 1　securengine 软件隐藏秘密信息前后 LSB 平面变化

2.3 统计检测

统计检测中最为著名的就是 x^2 统计检验法[2]和 RS 统计检验法[3]。其中 x^2 统计检验法思想是当加密信息以 LSB 方式嵌入图象掩体时将导致隐写载体相邻色彩索引值或相邻 DCT 系数出现的频率趋于一致的统计特征，通过统计量 x^2 来度量这个特征从而判断有无隐藏信息。

RS 统计检验法思想是通过分析无损隐藏容量来检测信息。无损隐藏容量是指 LSB 的隐藏容量减去用于恢复图象掩体而保存的相关信息后剩下的容量。随机改变 LSB 会减小最低比特位平面的无损隐藏容量。对于大多数图像掩体，在最低位隐藏随机信息会增大像素值的波动。据此可以把像素组分成三类：

规则像素组：随机改变 LSB 使其波动程度增大；

异常像素组：随机改变 LSB 使其波动程度减小；

无用像素组：波动程度不受随机改变 LSB 的影响。

对于图象掩体正反随机改变 LSB(1 - >0 或 0 - >1) 基本不影响规则像素组和异常像素组数目，但是对于隐藏载体，正反随机改变 LSB 对规则像素组和异常像素组数目的影响却很大。RS 统计检验法正是利用这个结论来判断有无隐藏信息的。

2.4 通用盲检测

通用盲检测是一种不管使用何种隐藏算法都能通过训练隐藏前后图象来调整阀值门限的检测方法。比较典型的是图象质量回归分析法[4]和高阶统计量分析法[5]。图象质量回归分析法的思想是当信息隐藏到图象中后，必然引起图象质量的降质，利用度量图象质量 26 种指标的度量组合来记录图像的质量，然后依据对信息隐藏软件隐藏的图象进行参数训练的结果判断出图象中这些参数及其组合是否符合信息隐藏的特征。定义多元线性回归模型：

$$\begin{aligned} y_1 &= \beta_1 x_{11} + \beta_2 x_{12} \cdots\cdots \beta_q x_{1q} + \varepsilon_1 \\ y_2 &= \beta_1 x_{21} + \beta_2 x_{22} \cdots\cdots \beta_q x_{2q} + \varepsilon_2 \\ y_n &= \beta_1 x_{n1} + \beta_2 x_{n2} \cdots\cdots \beta_q x_{nq} + \varepsilon_n \end{aligned} \quad (1)$$

其中 $x_{ij}(i,j \in [1,2\cdots\cdots q])$ 为质量度量值，下标 i 表示第 i 张图象，下标 j 表示质量度量值，总个数为 q，ε 为随机产生的误差，$y_1 y_2 \cdots\cdots y_n$ 表示量化的回归值，β 表示回归系数，其值通过最小均方误差(MMSE)预测器来获得。算法首先根据式 1 通过训练图象库得出回归系数 $\hat{\beta}$，再对待检测的图象进行滤波得到滤波前后图象质量值由式 2 得出 $\hat{y}$。

$$\hat{y} = \hat{\beta}_1 x_1 + \hat{\beta}_2 x_2 \cdots\cdots \hat{\beta}_q x_q \quad (2)$$

取判决门限 =0，当 $\hat{y} \geq 0$ 图象含有隐藏信息，当 $\hat{y} < 0$ 时，不含隐藏信息。

高阶统计量分析法的思想是利用图象的 n 级小波分解来构造统计特征向量，再根据特征向量判断有无隐藏信息。算法首先用 $v_i(x,y)$，$H_i(x,y)$，$D_i(x,y)$ 代表在尺度 i 的垂直、水平和对角子带，再对所有的 i =1，

2,...,n-1 计算所有三个子带的前四阶矩得出 12(n-1)个统计量包括峰值、偏度等,然后使用最佳线性预测器从空间性、方向性和相邻尺度收集了实际的小波系数值与最佳预测器的预测误差并计算误差分布的最初四个矩作为特征向量的另一部分。整个过程就是对所有水平与垂直子带的 n-1 个尺度重复处理。因此,最后的特征向量长度就是 12(n-1)+4*3(n-1)=24(n-1)。最后使用菲希尔线性鉴别将特征向量分为两簇以阀值来划分是否含有隐藏信息。

3 算法的分析与评价

图象信息隐藏检测研究属于交叉学科领域,从简单的视觉检测到复杂的通用盲检测涉及到了计算机图象学、软件分析、数理统计、图象处理、信号分析和密码分析等理论的应用。视觉检测对空域连续嵌入或非饱和随机嵌入都有好的检测效果,但是对于压缩域和频域的嵌入,人眼将无法辨别出隐藏信息的存在而且不能实现因特网信息隐藏图象自动化的检测,所以视觉检测在工程实践中很难发挥效用。特征码检测尽管检测成功率相当高而且很容易工程化,但是新近发布的商业隐藏软件几乎不再含有特征码,制约了特征码检测的应用范围。统计检测是图象信息隐藏检测中最常用也是最有效的方法。x^2 检验法可以估计出嵌入信息长度和位置,但是要求秘密信息的嵌入是按顺序的,当图象载体的颜色频率成分丰富、嵌入信息是非顺序且不符合均匀分布时检测准确率将大大下降。相反 RS 检验法则对越随机嵌入的信息检测效果则越好。但该方法完全将嵌入信息当作噪声,覆盖图像初始偏差、噪声级别等都会对估计精确性产生影响。表 1 给出了典型统计检验方法 RQP[6]、JPGCOM[7]、x^2 和 RS 检测适用范围的比较。

表 1　典型统计检验方法 RQP、JPGCOM、x^2 和 RS 检测适用范围的比较表

检验方法	RQP	JPGCOM	x^2	RS
适用范围	24BIT 真彩 BMPLSB 随机隐藏图像	JPEG 生成图像	BMP 调色板图像、GIF 图像调色板、JPGDCT 系数顺序隐藏	彩色和灰度 BMPLSB 随机隐藏图像

从表 1 中可以看出统计检测都有自己的检测适应范围,一旦超出检测范围检测性能将严重下降。在工程应用中由于事先无法知道隐藏的方式因此统计检测也有一定的局限性。

图象质量回归分析是典型的通用盲检测算法,对于在空域或压缩域的已知和未知的隐藏算法都有普遍的适用性,但是检测的准确率直接决定于图象数据库中对图象质量度量指标的训练结果,可靠性和精确性有限而且算法实现的工作量较大。高阶统计量分析算法是建立在图象像素或 DCT 系数隐藏等一阶统计特性的分布变化之上的,因此对信息隐藏的检测具有广泛的适用性但是算法对嵌入容量有严格的要求即隐藏信息长度大于图象掩体数据长度的 1/16 时才可能得到较好的效果。表 2 给出了隐藏容量在 20%-80% 之间标准图象库下图象质量回归分析和高阶统计量分析的平均正确检测率。

总之,从当前的检测方法研究情况来看每种检测方法都有自身的优缺点和使用范围,从计算机工程实践角度来看没有一种检测方法在实际的网络通信环境中检测准确性高于 80%,怎样提高图象信息隐藏的检测准确性将是科研攻关的重点。

表 2　标准图象库下图象质量回归分析和高阶统计量分析的平均正确检测率

检测算法	steganos	stools	Jsteg
图象质量回归分析法	70% 左右	75% 左右	70% 左右
高阶统计量分析法	60% 左右	75% 左右	80% 左右

4 算法研究的难点

因特网上 JPG 图象占所有静止图象的 70%,因此检测 JPG 图片是信息隐藏研究的主要方向之一,但是 JPG 图象格式本身十分复杂、信息隐藏在变换域中进行和隐藏算法安全性的不断提高给基于 JPG 图象隐藏检测带来了巨大困难。首先是早期的 JSTEG 隐藏算法,它将秘密信息未加密的隐藏在 DCT 系数的 LSB 上,再是 JPHS 算法将秘密信息加密后隐藏在 DCT 系数的

LSB 上，然后是 F5 算法将 DCT 系数上隐藏的加密信息比特进行交换，最后是 OUTGUESS 算法，为了防止统计检测该算法对修改的 DCT 系数的 LSB 而引起的与图象掩体 DCT 系数的统计变化进行了统计补偿以消除这种改变使得高准确率的检测变得几乎不可能。另外，信息进行了加密也是检测中的难点，象国产的 HIDE 软件，该软件嵌入时直接将 DCT 系数的 LSB 按规则修改为加密的秘密信息提取时直接对这些比特按规则组合并解密，如果解密结果是明文则判断为隐藏的信息，如果是乱码则判断为无隐藏信息。由于检测算法没有密钥，即使提出了大部分加密的秘密信息也根本无法解密得出准确的判断结果。目前对 JPG 的检测主要有效的办法仍然是统计检测，研究能够准确检测最新的 JPG 隐藏算法的统计方法将是当前算法研究的难点。

5 算法的研究方向

一种是根据统计检测的思想寻找新的能够准确度量隐藏前后载体特征的统计量。在 BMP 图像中相邻像素差值的直方图服从正态分布隐藏信息后将服从近似正态分布；在 GIF 图像中隐藏信息后的调色板的色彩值相近值对会有所增加；在 JPEG 图像中隐藏后的 DCT 系数的频率值会成对出现；怎样利用以上基本规律建立一个合适统计量能使检测成功率大大提高是下一步算法研究的方向之一。隐藏信息的过程就是向图像掩体中加入噪声的过程，Lapalace 变换是一种高通滤波的方法，因此对于隐写载体如果能准确度量 Lapalace 变换后直方图的变化将得到高的准确检测率。类似 Lapalace 变化如果图象掩体看成一个原始的信息空间而将隐藏载体看成隐藏信息后的空间，那么现有的隐藏方法包括 FFT、DCT、DWT 等都可看成原始图象空间到隐藏图象空间的算子，那么已知隐藏算子自然可以通过其逆算子将隐藏信息检测出来。但是实际情况是检测者不知道对方采用了什么算子对秘密信息进行了处理，这就是检测的困难所在。那么要想作到检测可能应该努力寻找另一个算子使得隐藏前后具有明显统计规律差异从而准确检测。

6 结束语

目前世界上已经有许多学者和研究机构致力于对图象信息隐藏检测研究之中，但是至今还未形成一套完整的理论关键的难点还没有实质性的突破，现有检测算法的准确率、适用性都有待进一步的发展和完善，因此图象信息隐藏算法的研究将向两个方向发展：其一是开发更加精确、快速、可靠的检测算法，其二是分析比较当前所有有效的检测算法，找出各自的优点、局限性和适用范围，将所有这些算法集成一个分析系统，对构成系统的所有检测算法扬长避短，从而大大提高系统的检测准确性。系统集成可以基于两种策略：一种是对检测载体综合应用各种分析算法，再对所有检测结果进行分析，根据人工智能得出判断结果；另一种是建立一个分析系统，在系统中调度不同的检测算法检测不同统计特性的检测载体，达到检测算法与检测载体的最佳匹配，从而提高系统的检测准确性。

参考文献

1 王炳锡等，数字水印技术，西安电子科技大学出版社，2003。

2 Andreas Westfeld, Andreas Pfitzmann: Attacks on Steganographic systems in Andreas Pfitzmann (Ed): Information Hiding Third International Workshop , LNCS 1768, Springer – Verlag Berlin, Heidelberg ,2000, pp ,61 –76.

3 Fridrich Jessica, Golian Miroslav, Du Rui. Detecing LSB steganography in color and gray – scale images IEEE Tranaction on Multimedia, 2001, 8(4): 22 ~ 28.

4 Avcibas I, Memon ND, Sankar B. Steganalysis based on image quality metrics. In: Dugelay j – l, Rose K, eds. Proc of the IEEE 4th Workshop on Multimedia Signal Processing Canners: IEEE, 2001, 517 – 522.

5 H. Farid, "Detecting Steganograhpic Message In Digital Images ", Report TR2001 – 412, Dartmouse college, hanover, NH, 2001.

6 J. Fridrich, R. Du, and L. Meng, " Steganalysis of lsb Encoding in Color Images" Proceedings IEEE International Conference oj Multimedia and Expo, July 30 – Auguest 2, 2000, NewYork City, Ny.

7 J. Fridrich, M. Goljan, andD. Du, " Steganalysis based on JPEG Compatibility" SPIE Multimedia systems and Applications IV, Denver, Co, August 20 – 24, 2001.