

隐写分析算法的量化评估方案

邓诗智 刘九芬 张卫明

(解放军信息工程大学信息工程学院, 郑州 450002)

摘要: 根据隐写分析算法的特点和应用需求, 结合 ROC分析, 提出了一个隐写分析算法的量化评估方案。包含 4个评估指标, 涉及算法的可靠性和准确性、适用性、分类代价和计算复杂度。并研究算法达到有效检测时, 对应载密对象的最小嵌入率, 分析了影响计算复杂度的因素, 提出了样本量分析, 并针对实际应用对虚警率和漏报率的不同需求, 提出了分类代价分析。量化评估结果对于改进和应用算法具有参考意义, 根据结果可以对算法的优劣进行多方面的比较, 从而确定出最优的算法。

关键词: 算法评价; 隐写分析; ROC分析; LSB替换

中图分类号: TP391 **文献标识码:** A **文章编号:** 1001—0505(2007)增刊(I)-0076-05

Scenario of quantitative evaluation for steganalytic algorithms

Deng Shizhi Liu Jiufen Zhang Weiming

(Information Engineering Institute PLA Information Engineering University Zhengzhou 450002 China)

Abstract According to characteristics of steganalytic algorithms as well as the need of application, a scenario of quantitative evaluation is put forward combining receiver operating characteristic (ROC) analysis. The scenario contains four evaluation rules relating to reliability and veracity, applicability, classifying cost and computing complexity of steganalytic algorithms. Minimum embedded ratios which algorithms can detect efficiently and the factor which influences computing complexity of algorithms are discussed. Accordingly, analysis of sample size is advanced. To adapt different requirement in false alarm rate (FAR) and false detection rate (FDR), analysis of classifying cost is also put forward. Evaluation results are good reference to apply and improve steganalytic algorithms. Furthermore, the results can be used for comparing algorithms different sides so that the best algorithm can be determined.

Key words: arithmetic evaluation, steganalysis, receiver operating characteristic (ROC) analysis, least significant bit (LSB) replacement

信息隐藏作为信息安全领域的一个新的前沿技术, 已经成为信息技术领域研究的热点。数字隐写(steganography)和隐写分析(steganalysis)是信息隐藏技术的重要分支。前者是将秘密消息隐藏在载体中进行传送而不引起第三方怀疑, 达到隐蔽通信的目的。后者是对隐写的攻击, 即检测、提取、还原。破坏隐藏的保密信息。隐写已成为保密通信的有效手段, 但隐写也会被敌对势力利用, 成为危害国家政治、经济安全的工具(媒体对此已有诸多的报道)。目前互联网上已经出现了两百多种隐写软件, 而且利用这些软件不需要高深的专业知识。因此隐写分析是一个紧迫的研究领域。

到目前为止, 在隐写分析领域中开展的研究基本上集中于对隐蔽信息的检测, 并且已经提出了大量的隐写分析算法。一方面, 由于受实验环境的限制, 当前各种各样的隐蔽信息的检测方法往往只是对几幅、几十幅或者几百幅图像进行实验验证。由于图像的多样性和复杂性, 这样的实验结果往往是不可靠的。另一方面, 不同的应用需求对隐写分析算法的性能的要求也不相同。量化评估这些算法不仅可以得到算法在不同指标上的性能, 还可以揭示算法的不足, 从而提供改进方向。进一步, 根据实际应用需求, 选择最佳的算法或者算法集合进行隐写分析。

郎荣玲等^[1]就算法的适用范围对分辨函数^[2]、卡方检验^[3]和 RS^[4]算法进行了分析,结论是:前 2 种算法适用于嵌入的秘密信息为均匀分布、嵌入算法为 LSB 替换连续嵌入的情况,而 RS 算法则没有这些限制。Ker^[5-6]把图像分成自然图像和经过 JPEG 图像转化来的空域图像 2 种类型,按照图像类型和图像大小建立四类图像库,用 ROC 曲线图分析实验结果,讨论了 Pairs^[7]算法、RS 算法^[4]和 SPA^[8]算法的可靠性。

本文根据隐写分析算法的特点和实际需求提出一个量化评估方案,方案包括 4 个量化评估指标和具体的实现方法,分别为准确性和可靠性、适用性、分类代价和计算复杂度。这些指标中,第一个指标适合于可以估计嵌入率大小的隐写分析算法,其余指标所需的数据仅为隐写分析算法判断检测对象隐写与否的结果,故适合于所有的隐写分析算法。

1 隐写分析算法的量化评估方案

1.1 可靠性和准确性

定量隐写分析算法是可以估计嵌入秘密信息长度的隐写分析算法,可以计算出隐写对象中含有秘密信息的大小,即对应秘密信息的嵌入率大小。这些算法实际上都是构造一个估计嵌入率的统计量,其中统计量的无偏性、有效性和一致性是经常被讨论的指标。由于嵌入率估计值的平均大小和离散程度是表征算法检测效果的主要指标,也是指导应用算法的重要依据,而一致性主要讨论统计量的收敛性。因此本节讨论统计量的无偏性和有效性。

以算法得到的嵌入率估计值和真实值的差为评价对象,本文提出以下 2 个指标:

1) 可靠性:表征算法对嵌入率估计值的离散程度或平稳程度,用于度量统计量的优效性。采用标准差来衡量统计量的可靠性。

2) 准确性:表征算法对嵌入率估计值的准确程度,用于度量统计量的无偏性。采用均值来衡量统计量的准确性。

可靠性表征了定量隐写分析算法检测不同对象时的稳定程度,准确性表征了算法检测不同对象时的准确程度。

当检测对象例如数字图像类型纹理等比较复杂时,算法的可靠性是首先需要考虑的问题,因为只有可靠性高的算法才能保证检测结果具有较高的可信度。在某些情况下,例如研究某类隐写术的提取工作过程中,针对检测对象,提取算法需要得到较准确的嵌入率大小,从而降低提取工作的计算复杂度。此时准确性就是需要着重考虑的指标。

1.2 适用性

隐写分析算法的一个重要目的是检测可疑对象是否隐藏有秘密信息,而可疑对象形式多样,一般由载体对象、隐写算法和隐写内容等因素确定。为了考察隐写分析算法对不同检测对象的适用程度,本节提出适用性指标:算法对某类隐写对象的适用性用对应的检测效果表示,隐写分析算法可以有效检测的载体对象种类越多,其适用性就越好。其中检测效果用 ROC 分析中的全局检测率(AUC)表示,规定算法达到有效检测指的是全局检测率大于等于 0.85。

在分类问题中,常用的分析方法是 ROC(receiver operating characteristic)分析^[9],描绘虚警率和检测率两者关系的曲线称为检测器接收操作特性(ROC)曲线。在 ROC 分析中,全面衡量分类效果的一个量称为全局检测率,其大小用 ROC 曲线图与横坐标包含区域的面积 AUC(area under curve)表示。具体定义为

$$P_t = 1 - P_e \quad (1)$$

式中, P_e 为平均错误概率,其定义为

$$P_e = \alpha P_{\text{cover}} + \beta P_{\text{stego}} \quad (2)$$

式中, P_{cover} 和 P_{stego} 分别表示从检测对象中取到载体和载密的概率; α 表示虚警率; β 表示漏报率。

上述的隐写对象,一般由以下几个因素共同决定而成:

1) 隐写算法。嵌入秘密信息时所采用的隐写规则,其中包含可能使用的隐写密钥,常见的隐写算

文本和视频等。图像由于应用的广泛性，已经成为最常用的隐写载体之一。隐写载体的统计特征往往呈现出多样性，比如 BMP灰度图像，可以按纹理复杂程度分类，也可以按图像的大小来分类。

3) 隐写消息。隐写消息就是嵌入到载体中的秘密信息，它的主要特征是其分布和数据长度。一般情况下，隐写时采用的秘密信息服从一定的概率分布，比如两点分布、高斯分布等。

通过上面3个因素的两两组合，可以得到不同类型的检测对象。针对不同的检测对象，利用隐写分析算法的检测结果进行ROC分析，并计算出全局检测率AUC。AUC的数值就量化表征了算法对此类对象的适用性程度，若达到有效检测，即若AUC大于等于0.85，则算法适用于检测此类载密对象。隐写分析算法的适用性就用达到有效检测的对象数量来表示。

另外，由于隐写对象的嵌入率是影响检测效果的重要因素，一般嵌入率越小，对应隐写对象的修改量就越小，隐写分析算法对其的检测效果越差。

本文定义隐写分析算法能检测的最小嵌入率为：算法达到有效检测时对应隐写对象的嵌入率大小。隐写分析算法的最小嵌入率的大小表征有效检测的嵌入率范围，是考虑算法适用性时必须考虑的一个问题。

根据算法的检测性能，嵌入率在选取的合适范围内变动，如嵌入率变化区间为[0, 0.1]，这个嵌入率区间被分成 k 等分，其中 k 的选取根据所需精度确定，实验表明，一般取 $k=10$ 可以得到较准确的估计。依次选择 k 个嵌入率，利用算法的检测结果分别进行ROC分析，得到 k 组嵌入率与AUC的数据。实验发现AUC与嵌入率的关系可以用多项式函数较好地拟合，根据拟合数据，对应AUC等于0.85的嵌入率，就是隐写分析算法能检测的最小嵌入率。

1.3 分类代价分析

根据1.2节的分析，全局检测率AUC衡量着隐写分析算法的分类效果，但是1.2节全局检测率的计算公式并没有涉及虚警率和漏报率的权值大小，此时假设的是虚警率和漏报率造成的代价是相同的，其中虚警率的代价指资源花费，漏报率的代价指信息损失。例如网络环境下的一个实时检测系统，每天处理可疑对象的数据量很大，一方面，若算法的虚警率较高，将产生大量载体对象用于进一步处理，极大地占用存储空间和计算资源，此时虚警率造成的代价就是这些无意义的资源花费；另一方面，若算法的漏报率较高，将会遗漏掉很多载密对象，可能造成重要价值的信息损失。

根据实际应用对资源花费和信息损失的不同要求，全局检测率已经无法准确判断算法在实际情况下的分类效果。基于此，本节提出了分类代价分析，可以得到对虚警率与漏报率的不同要求下，隐写分析算法花费的代价。根据分类代价分析可以得到隐写分析算法对应的代价变化情况，从而选择代价最小的算法进行检测。代价最小的算法所对应的资源花费与信息损失达到合适的折中。

类似Drummond等^[12]提出的COST分析，定义以下2个概念：

1) 概率花费函数 (probability cost function, PCF)

$$PCF(+)=\frac{P(+)\mathcal{C}(-|+)}{P(+)\mathcal{C}(-|+)+P(-)\mathcal{C}(+|-)} \quad (3)$$

式中， $\mathcal{C}(+|-)$ 和 $\mathcal{C}(-|+)$ 分别为虚警率和漏报率的代价， $P(+)$ 和 $P(-)$ 分别为取到载密和载体的概率。类似地可以定义 $PCF(-)$ ，且有 $PCF(+)+PCF(-)=1$ 。设 $\eta=\frac{\mathcal{C}(+|-)}{\mathcal{C}(-|+)}$ ，则 PCF 的定义转化为

$$PCF(+)=\frac{P(+)}{P(+)+\eta P(-)} \quad (4)$$

2) 正规化期望代价 (normalized expected cost, NEC)

$$\mathcal{C}_{NE}=(1-P_T)\times PCF(+) + P_F \times PCF(-) \quad (5)$$

式中， P_T 和 P_F 分别为ROC曲线的一个点对应的检测率和虚警率， \mathcal{C}_{NE} 表征了已知某个确定的虚警率和漏报率时，花费与 η 的关系。因为 $PCF(+)+PCF(-)=1$ ，故 \mathcal{C}_{NE} 转化为

$$\mathcal{C}_{NE}=(1-P_T-P_F)\times PCF(+) + P_F \quad (6)$$

根据式(4)和(6)，以 PCF 为横坐标，以 \mathcal{C}_{NE} 为纵坐标作图，得到的就是分类代价图，反映了随着虚警

1.4 计算复杂度分析

隐写分析算法的计算复杂度是一个重要的评价指标,一般分为时间复杂度和空间复杂度,分别影响着算法的运行速度和存储空间。例如在网络环境下处理大流量数据时,计算复杂度高的算法会严重降低资源利用效率,甚至导致算法的应用失败。本节主要考察隐写分析算法的计算复杂度。另外,通过分析影响计算复杂度的因素,本文提出了样本量分析,它可作为一种降低计算复杂度的方法。

1.4.1 时间复杂度

隐写分析算法的时间复杂度指的是算法在处理数据过程中所需要的时间。可通过分析算法的实现步骤从而计算得到,以计算机中的最小处理单元位操作数目为单位。

1.4.2 空间复杂度

隐写分析算法的空间复杂度指的是算法在处理数据过程中所占用的存储空间,即所需的内存大小。空间复杂度是通过分析算法实现步骤计算得到,以字节(byte)为单位。

1.4.3 样本量分析

影响计算复杂度的因素分析:在研究计算复杂度的过程中,作者发现:当隐写分析算法确定后,其计算复杂度的高低主要与待检测对象的大小有关。以数字图像为例说明,隐写分析算法的计算复杂度随着图像尺寸的减小而降低。

既然检测对象的大小决定了计算复杂度的高低,为了降低隐写分析算法的计算复杂度,可以取部分图像数据代替整幅图像,作为隐写分析算法的输入。同时,减少输入的样本量会导致检测效果的降低,为了找到计算复杂度和检测效果两者之间的折中点,考察样本量与检测效果的关系,并提出了下面的样本量分析。

样本量分析是在保证检测效果的情况下,尽可能地降低用于检测的数据样本量,同时保证一定的检测效果。定义隐写分析算法能检测的最小样本量为:算法达到有效检测时,对应载密对象的样本量大小。

以上分析也就解释了 Kett^{5,6}的结论:针对同一个隐写分析算法,实验不同尺寸的图像得到的检测效果也不相同。即针对相同类型的图像,其尺寸越小,检测效果越差。

样本量分析:将样本量分成 n 等分,其中 n 根据所需结果的精度确定,一般取 $n=10$ 可以得到较准确的结果,类似 1.2 节算法能检测的最小嵌入率的计算过程,依次累加样本量,得到 n 组样本量和全局检测率 AUC 的数据。实验发现,样本量和 AUC 的关系可以用多项式函数较好地拟合,根据拟合数据计算出对应 AUC 为 0.85(实际应用时可以根据实际对检测效果的需求重新定义 AUC 值)的样本量,这个样本量的就是隐写分析算法能检测的最小样本量。

2 应用评估结果

应用隐写分析算法的量化评估方案,依据得到的评估结果,按照实际需求选择最合适的算法进行检测:当需求比较单一时,如只考虑算法的准确性或适用性等,根据评估结果,可以很容易地选择最优的算法;当需求不单一时,如网络环境下的快速检测,此时需要根据不同的需求,动态地确定每个指标的重要性程度,如采用层次分析法^[13]从而得到最优的算法或算法集合,这也是以后工作的方向。

3 结语

本文提出了一个隐写分析算法的量化评估方案,方案包含 4 个评价指标和具体实现方法。应用评估方案,对隐写分析算法进行了不同方面的比较,可以确定最优的算法。值得一提的是,方案采用 ROC 分析,所需的数据仅为算法判断对象隐写与否的分类结果,故适用于所有的隐写分析算法。

本文根据隐写分析算法的特点和实际的需求提出一个量化评估方案,随着应用和研究的深入,更多合适的量化评估指标是可以考虑的问题。未来的研究方向是如何充分利用得到的这些算法评价结果,针对不同的隐写对象,给出一个最优的检测方案。

- Lang Rongling Xia Yu Zhi Yan et al. Analysis and evaluation of several typical steganalysis algorithms [J]. Journal of Image and Graphics, 2004, 9(2): 249-256. (in Chinese)
- [2] Lee Y K Chen L H An adaptive image steganographic model based on minimum error LSB replacement [C] // IEEE Proceedings of the Ninth National Conference on Information Security. Taichung, 1999: 8-15.
- [3] Wesfrid A Pfitzmann A Attacks on steganographic systems [C] // Proceedings of Third International Workshop Berlin, 1999: 61-75.
- [4] Fridrich J Goljan M Du R Reliable detection of LSB steganography in grayscale and color images [C] // Proc of Special Session on Multimedia Security and Watermarking. ACM Press, 2001: 27-30.
- [5] Ker Andrew D Quantitative evaluation of pairs and RS steganalysis [J]. Proceedings of SPIE, 2004, 5306: 83-97.
- [6] Ker Andrew D Improved detection of LSB steganography in grayscale images [C] // Proc of the 6th Information Hiding Workshop Berlin, 2004: 97-115.
- [7] Fridrich J Goljan M Soukal D Higher order statistical steganalysis of palette images [C] // Proceedings of Electronic Imaging. SPIE Press, 2003: 178-190.
- [8] Dumitrescu S Wu X Wang Z Detection of LSB steganography via sample pair analysis [J]. IEEE Transactions on Signal Processing, 2003, 51(7): 1995-2007.
- [9] Bradley A P The use of the area under the ROC curve in the evaluation of machine learning algorithms [J]. Pattern Recognition, 1997, 30(7): 1145-1159.
- [10] Hirohisa H Iokji A data embedding method using BPCS principle with new complexity measures [C] // Proc of Pacific Rim Workshop on Digital Steganography. Kitakyushu, Japan, 2002: 30-47.
- [11] Marvel LM Boncelet CG Retter CT Spread spectrum image steganography [J]. IEEE Transactions on Image Processing, 1999, 8(8): 1075-1083.
- [12] Drummond C Holte R Explicitly representing expected cost: an alternative to ROC representation [C] // Proceedings of Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM Press, 2000: 198-207.
- [13] 张伟, 郭捷, 陈克非. 隐写分析算法的模糊综合评估 [J]. 计算机工程, 2006, 32(21): 141-144.
Zhang Wei Guo Jie Chen Kefei Fuzzy comprehensive evaluation of steganalysis algorithms [J]. Computer Engineering, 2006, 32(21): 141-144. (in Chinese)