基于大数据环境的多模态信息隐藏新体系

黄殿中[1],张静飞[1],张 茹[2],李鹏超[3],郭云彪[3]
(1. 中国通用技术研究院,北京 100192; 2. 北京邮电大学网络空间安全学院,北京 100876;
3. 北京电子技术应用研究所,北京 100091)

摘 要: 信息隐藏研究经过数十年的发展,在隐写术和隐写检测方面都积累了大量成果,但是信息隐藏的应用目前仍局限于实验室研究,聚焦于发现与抗发现的对抗,距实际应用仍有一定的距离. 论文在对当前信息隐藏研究深入分析的基础上,借鉴密码学思想,提出建立适应于当前大数据环境,算法可变、修改模式可控的抗取证信息隐藏系统;通过全面整合信息隐藏算法和嵌入修改模式,构建多模态信息隐藏技术空间,实现用户通过输入密钥参与信息隐藏处理控制的全新研究思路和应用方式. 论文通过理论分析和实验初步验证该系统的有效性和安全性.

关键词: 信息隐藏; 隐写; 抗取证信息隐藏; 多模态信息隐藏
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2017)02-0477-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.02.029

New System of Multi-modal Information Hiding Based on Big Data Environment

HUANG Dian-zhong[1], ZHANG Jing-fei[1], ZHANG Ru[2], LI Peng-chao[3], GUO Yun-biao[3]
(1. *China General Technology Research Institute, Beijing* 100192, *China*;
2. *School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*;
3. *Beijing Institute of Electronics Technology and Application, Beijing* 100091, *China*)

Abstract: A large amount of achievements have been accumulated in steganalysis and steganography community for the past few decades. Nevertheless, the application of information hiding is restricted to research in laboratory, focusing on the confrontation between steganography and steganalysis, which has a huge distance from real world. Inspired by the cryptography, we establish a novel information hiding system whose algorithms are changeable and modification modes are under control based on investigation of previous work. We construct a huge multi-modal information hiding space with multiple algorithms and modification modes. Moreover, we build the mapping method between steganography methods and keys to implement the reconstruction mechanism of generating information hiding process when giving a key. There is no doubt that information hiding research scope will be expanded and vitality will be integrated. Experimental results and theoretic analysis have shown that the proposed system is effective and security.

Key words: information hiding; steganography; anti-forensic information hiding; multi-modal information hiding

1 引言

随着大数据时代的来临,企业大数据、政府大数据、网络用户大数据等在各个行业发挥了巨大价值:它们能揭示其他手段看不到的新变化趋势,但同时人们的任何行为都可能被追踪、记录. 在大数据环境网络用户变成了透明人,安全门事件频出,人们对隐私保护的需求也日趋强烈. 信息隐藏技术是保障信息安全的重要手段,以"隐匿秘密通信存在"的方式来保护通信的安全,在隐私保护中发挥了重要作用. 隐藏技术不但可以像加密技术一样保护通信内容,还可以掩盖通信存在的事实. 然而信息隐藏并没有像密码学那样走进人们的计算机桌面,还仅限于实验室研究和专业应用,不能满足大数据时代的实际需求.

信息隐藏滞后于大数据时代主要源自三方面. 第一,信息隐藏研究聚焦于发现与抗发现的对抗研究中,

收稿日期:2016-06-27;修回日期:2016-12-07;责任编辑:诸叶梅
基金项目:国家自然科学基金(No. U1536207, No. U1536104);国家科技支撑计划项目(No. 2014BAH41B01)

而实际上抗发现信息隐藏实用性不足. 很多研究聚焦于单个隐藏技术与检测技术的博弈. 在考虑信息隐藏抗发现检测安全性时一般都有很多假设条件:假设已知用户采用的算法,已知载体的统计特征. 然而进入大数据时代,载体形式多样、来源广泛,依托大数据环境的信息隐藏有更广阔的发展空间.

第二,信息隐藏技术的抗取证安全性一般建立在算法保密的基础上,一旦和信息隐藏技术相关的先验知识(例如算法、载体统计特征、信道特征等)泄露,其安全性会受到严重威胁. 而大数据时代的开放性特点,使得大量公开的信息隐藏技术和应用暴露在大数据环境中. 假设检测者掌握了信息隐藏工具,这就意味着获取了隐藏通信的大量先验知识,在此基础上就可以进行机器学习和穷举攻击,进而直接获取证据性信息. 而对于一个普通使用者,只能利用公开研究成果,这样必然要考虑信息隐藏技术被检测者掌握的风险.

第三,现有信息隐藏用户参与度不够,普通用户无法确认隐藏技术的安全性. 与密码技术中使用者可通过输入密钥来参与加密过程不同,传统信息隐藏技术给使用者的直观感受是技术核心掌握在算法设计者的手中,使用者会很自然的想到隐藏的信息会不会被设计者提取出来. 相反,加密技术一般要求满足 Kerckhoffs 准则,即通信系统中使用的加密体制和算法应当是公开的,系统的安全性依赖于密钥的选取. 加密算法公开后,核心机密仍掌握在用户手中. 正是这种用户输入密钥的参与机制,使普通用户对密码的保护作用有信心.

为了解决信息隐藏在大数据时代不实用,不安全,用户参与度不够的问题,本文提出抗取证的多模态信息隐藏模型,充分利用信息隐藏多年来发展的成果,并利用大数据时代充斥于互联网中的多类型媒体信息、数据形式,借鉴密码学思想,构建一种能够满足 Kerckhoffs 准则、用户参与、算法可控、隐藏安全性可度量的多模态信息隐藏新体系.

本文接下来的内容包括以下几个部分:第二部分将回顾并分析抗发现信息隐藏近年来的成果和发展趋势,是本文研究内容的基础;第三部分针对抗检测信息隐藏的不足,提出抗取证的多模态信息隐藏模型;第四部分从抗发现和抗取证两方面,论述大数据环境下多模态信息隐藏模型的安全性;第五部分为结论和展望.

2 抗发现的信息隐藏研究

信息隐藏研究始于上个世纪 90 年代,一直在信息隐藏与隐藏分析的对抗中迅速发展. 然而目前信息隐藏研究发展速度有所放缓,信息隐藏技术研究难以突破 STC 框架,只是在失真函数方面做部分改进,这些改进多针对某些不足做修修补补,很难对隐藏性能带来较大的提高. 隐藏检测单纯靠增加特征维数或采用新的分类工具,对检测性能的提高贡献有限;并且隐藏检测有很多不满足实际应用的假设,检测的结果只是一个统计异常出现的概率,不能布控于实际网络来检测基于信息隐藏的隐蔽通信. 信息隐藏研究需要注入新的激励,跳出当前的发现与抗发现对抗发展逻辑,面向时代和环境的发展变化,推出抗破译安全性概念,研究面向实际应用的信息隐藏新体系.

前期的信息隐藏在理论研究、隐藏算法及载体、信息隐藏检测等研究方面取得了长足进步,为信息隐藏体系创新研究奠定了基础. 隐写编码作为增强信息隐藏性能的关键技术,不但提高了信息隐藏的载密效率,更重要的是为动态可控信息隐藏提供了大量可变的修改模式,为本技术提供了技术支撑. 接下来将从理论研究、隐藏算法及载体、信息隐藏检测和隐写编码四个方面简要分析信息隐藏的相关进展.

2.1 信息隐藏理论

信息隐藏理论研究主要集中在应用信号处理理论、概率统计理论、信息论、博弈论等相关理论来描述信息隐藏[1,2],对其安全性给出了定量或定性演绎,并在一定条件下探讨了安全隐藏容量边界. 在信息隐藏容量方面,CostaM、CohenA、LapidothA、MoulinP 等设计了许多经典模型[3]. 在安全性分析方面,Cachin[4] 等人认为一个隐写系统的存在安全性意味着载体和隐写后的统计分布在统计意义下的不可区分,提出利用 KL 散度(Kullback-Leibler Divergence) 度量两种分布的差异,用于衡量信息隐藏系统安全性. Pevny 等[5] 利用最大均值差(Maximum Mean Discrepancy)提出根据大量载体图像进行隐写安全性评估的方法,与 KL 散度相比,最大均值差异更易于计算、且在高维空间比较稳定;此外还有利用 Fisher 信息量给出安全嵌入容量并对其进行优化[6,7]. 文献[8 ~ 10]证明了多载体安全嵌入容量与载体数量的平方根成正比,单载体安全嵌入容量正比于载体尺寸的平方根. 然而像密码学那样,针对穷举攻击的破译对抗,基于运算复杂度的隐藏安全性研究成果并不多见.

2.2 隐藏算法和载体

公开文献记载的信息隐藏算法超过 300 种,大多数是单载体隐藏算法,例如 LSB 隐写、OPA 隐写、JSteg、OutGuess、F5 等[11,12],其统计特征异常易于检测. 有些学者针对特定统计分析对隐藏思路进行了改进,张涛等[13] 提出改变 LSB 嵌入方式和利用矩阵编码的安全性增强方法,Solanki 等提出能抵抗 JPEG 类隐写分析算法的 YASS 算法[14] 及其改进方案,Luo 等提出安全性增强了的 PVD 方法[15] 等. 这类方法的实现过程是针对特定隐写分析算法而改进原隐写方法,所以理论上讲其所

提高的安全性是有限的. 当前主流的方法主要是采用能够降低修改量的隐写编码方法,或者维持隐写前后统计特性不发生变化的统计保持方法. 关于隐写编码方法,后续将重点阐述. 这里着重介绍统计保持的隐写算法,如 Salle 提出的 Model-Based 方法[16,17]利用熵解码实现嵌入数据和载体数据分布的一致性,Amin[18]提出基于扩频的统计安全嵌入算法等等;也有针对载体高阶统计特性保持的研究,如 Sarkar[19]提出使用部分图像分块 DCT 变换系数,对嵌入时统计特性的改变进行补偿的二阶保持隐写算法;以及文献[20]中提出的保持频域高阶统计特性不变的隐写算法. 文献中还有许多类似的方法,但不管是对抗专用隐写分析的方法还是统计保持的方法都还存在一些需要改进的地方,具体表现在缺乏综合考虑隐写三要素——隐写容量、统计安全性和感知失真.

此外,多载体和无载体的研究也逐渐兴起. A. D. Ker 等[21]人深入研究了多载体隐藏策略;文献[22,23]提出了基于载体合成的信息隐藏方式,文献[24]提出了基于纹理合成的载体构造式数据嵌入新思路,文献[25,26]则利用汉字的数学表达式提出了一种无载体的文本信息隐藏方法,采用隐藏信息映射算法,有效对抗现有隐藏检测手段. 这些成果对多载体信息隐藏具有重要指导意义. 丰富的算法为信息隐藏提供了大量不同的修改方法,为构造大量算法空间提供了基础支撑. 除了隐藏算法的选择外,如果我们将承载秘密信息的载体也作为一个可变量来考虑,那么算法的变化空间就更为丰富,这对实现满足 Kerckhoffs 准则的信息隐藏新体系无疑有积极意义.

2.3　隐藏检测技术

隐藏检测技术随着信息隐藏的发展也在不断进步,主要包括针对特定隐写的检测算法和通用型隐写检测算法. 早期的隐写检测一般针对特定算法的检测,例如,RS 检测方法可以实现对 LSB 算法的有效检测[27],检测者针对部分隐藏算法还可以进一步估计秘密信息嵌入量,隐写检测的准确性也不断提高[28,29]. 后续出现的 break F5 检测方法通过剪切图像实现了对原始图像统计特性的估计[30],对通用检测方法有很好的借鉴和指导作用. 通用型隐藏检测算法一般通过统计特征和机器学习分类实现[31]. 常用的统计特征非常多,例如二元相似性度量特征[32]、DCT 与马尔可夫特征[33,34]、小波系数特征[35]、SPAM 特征[36]、共生矩阵特征与标定特征[37,38]等. 分类方法包括神经网络[39]、支持向量机[40]等. 而隐写分析特征的高维化是近年来重要的发展趋势,特征维度已经达到数千甚至上万[41],有学者通过降维[42]等方法来解决计算量激增问题. 有学者通过分类结果加权集成来提高检出准确率[43]. 文献[44]提出预分类、后隐写分析检测的框架,依据图像固有特性划分子类,在不同子类中实现检测,大大提高了检出率. 针对采用多载体承载秘密信息的“批量隐藏(Batch Steganography)”,文献[45]尝试解决多参与者的联合分析(Pooled Steganalysis)问题. 此外,文献[46]提出将隐藏检测看作一种数字取证技术,扩展了隐藏检测的研究思路. 本文研究在主要考虑信息隐藏抗破译安全性的同时,也兼顾算法的抗发现性安全,保证信息隐藏系统的总体安全.

2.4　隐写编码

隐写码是从提高隐写嵌入效率需求中提出的一般性编码问题. Crandall[47]提出了最早的矩阵编码之后,陆续出现了一系列隐写编码方法,例如 Golay 码[48]、BCH 码[49]及 Running 码[50]等. 文献[51]给出了隐写编码在一定失真条件下的性能理论极限. 文献[52]利用低密度生成矩阵构造了性能接近理论极限的二元编码方法. 湿纸编码[53]可自由选择嵌入位置,接收方不必知晓嵌入位置也可提取秘密信息. 文献[54]结合湿纸编码构造了多层隐写编码方法 ZZW. 2010 年,Filler 与 Fridrich 提出了 STC(Syndrome Trellis Codes)编码[55]. 相较于其他隐写编码,STC 方法使得设计基于图像内容的自适应隐藏算法变得非常方便. 当前信息隐藏研究的一个热点集中于失真函数设计,以保持原始载体的统计特性,如 HUGO、WOW、UNIWARD、MiPOD 等[56-60]. 文献[61]将安全性度量指标 KL 散度表征为失真代价的函数,进而寻找最优失真代价的设计方法以期优化隐写安全性度量,本文也试图探索合理选择失真代价函数的理论依据和未来的发展方向. 隐写编码为信息隐藏提供了大量不同的修改的方式,在某种意义上为信息隐藏提供了大量的算法空间. 假如我们能够建立密钥与修改方式的一一对应关系,那么构建满足 Kerckhoffs 准则的信息隐藏新体系就成为可能.

综上所述,国内外研究者在信息隐藏理论、方法和技术方面已经取得了丰硕成果. 针对复杂网络态势和日益提高的存储和计算能力,密文提取和抗取证分析这些问题会日益受到人们的关注. 信息隐藏应该未雨绸缪,从体系、理论、概念上拓宽研究思路,研究能够面向实际应用广泛推广的信息隐藏系统.

3　抗取证的多模态信息隐藏模型

在大数据时代,媒体形式丰富多样,同时对抗中发展的信息隐藏技术涌现出一大批优秀算法;对载密效率的追求又催生了矩阵编码、BCH 编码、STC 编码等一系列隐写编码,派生出海量的嵌入修改模式. 可以把隐藏算法、隐写编码等因素作为用户控制信息隐藏的调节参数,复杂的参数变化为用户可调节控制提供了可

能. 如果能够设计一种涵盖信息隐藏各种载体(格式、文本、图像、音频、视频等)、算法、编码方法、信道特征可变可控的信息隐藏新体系,就能应对复杂网络环境中的实际应用.

一方面,层出不穷的修改模式、海量可变的隐写编码拓宽了信息隐藏算法空间. 另一方面,丰富的网络媒体、多载体组合、无载体载密丰富了信息隐藏技术的秘密信息的传递方式. 这种算法、载体、信道和编码等多种因素的不断扩展,决定了信息隐藏技术集在不断扩展. 只要该集合足够大,就可以抵抗算法泄露带来的安全隐患. 如果再建立起密钥到信息隐藏技术实现的对应关系,从密文提取攻击的角度考虑,可以认为该体系满足 Kerckhoffs 准则. 当然,在实际中,可供选择的网络媒体格式或者说载体类型是有限的,隐藏算法设计也受载体特点、特性的制约,但通过载体、算法、编码等多种因素的有机结合,并通过用户密钥控制机制,就能保证信息隐藏技术集的空间足够大,就能在一定程度上抵抗穷举攻击和取证. 由此,我们提出了基于用户密钥控制的多模态信息隐藏系统模型.

该系统参数多变,算法可控,用户参与并结合信道数据特征反馈,来确定信息隐藏的算法、编码、载体. 图 1 给出多模态信息隐藏系统的具体通信模型,描述多模态信息隐藏和提取的全过程.

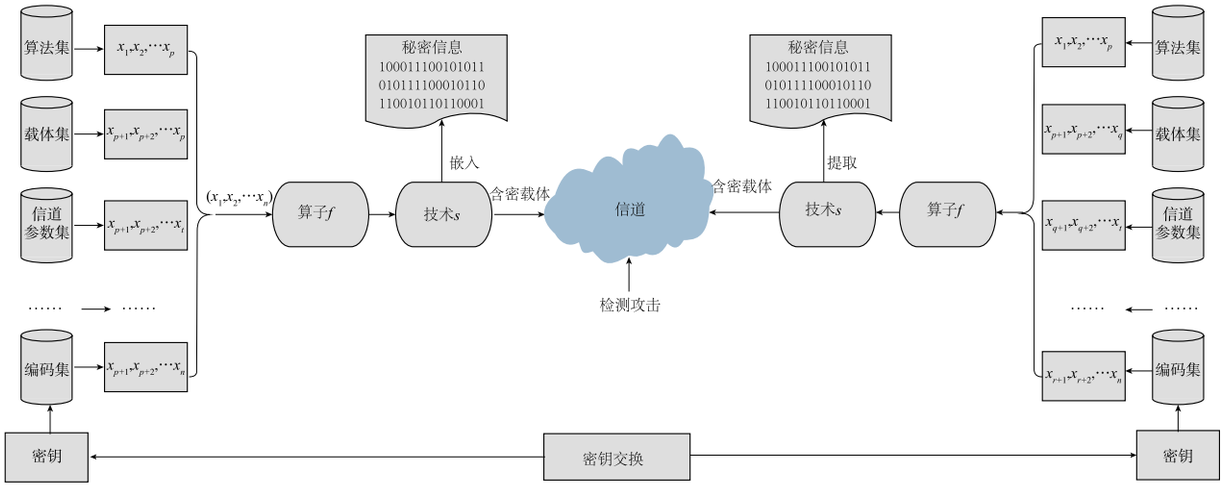

图1 大数据环境下信息隐藏系统模型

这里,我们可以把多模态信息隐藏系统抽象成一个线性空间. 我们定义$(x_1,x_2,\cdots\cdots,x_n)\in\mathbb{R}^n$为多模态信息隐藏系统影响因素向量,也是系统的输入向量. 信息隐藏技术实现的集合我们定义为$S=\{s_i\mid s_i=f(x_{i1},x_{i2},\cdots\cdots,x_{in})\}$,其中$s_i$对应第$i$次信息隐藏技术实现过程,$f$为信息隐藏生成算子,$(x_{i1},x_{i2},\cdots\cdots,x_{in})\in\mathbb{R}^n$是信息隐藏过程输入向量的第$i$次实现,向量的每个分量代表影响信息隐藏技术生成的某个因素,如采用的算法和载体等,总共有n维. 从图 1 我们可以看出,由于一次信息隐藏的实现可能采用多载体、多算法、多信道参数和多编码,因此算法集、载体集等因素可能对应多个维度. 假设,一个信息隐藏技术包含p个算法,对应输入向量中的前p项,$(x_1,x_2,\cdots x_p)$,同时在载体集中选择了$(x_{p+1},x_{p+2},\cdots x_q)$的载体,根据信道情况,适配选择信道参数$(x_{q+1},x_{q+2},\cdots,x_t)$,以及编码参数$(x_{r+1},x_{r+2},\cdots x_n)$等,这些变量都可由用户输入密钥控制. 所有这些影响因素的维度和是n. n越大,代表影响一次信息隐藏实现的因素越多,某一个分量的取值范围越大,某个影响因素的可能性就越多,这两个方面都决定多模态信息隐藏系统的安全性. 也就是说,控制信息隐藏n维空间的势决定了信息隐藏系统的抗取证安全性,这样信息隐藏和密码学一样,实现了基于计算复杂度的安全性定量度量.

为了抗取证,虽然很多情况在信息嵌入载体前,都会对密文进行加密预处理,密码与信息隐藏的结合无疑会增加技术的抗破译能力;然而这种抗破译能力是密码技术提供的,而非信息隐藏技术本身固有. 如果满足密文加密预处理带来的抗破译能力,那么信息隐藏只是为加密技术提供掩护的一种保护外壳(据此,很多不了解信息隐藏的密码专家认为信息隐藏技术不属于科学),很难成为与密码并列的信息安全支撑技术. 所以信息隐藏研究不但要隐藏秘密通信的存在,还要提高自身的抗破译能力. 再者信息隐藏前对密文进行加密预处理,让密文具有单一的伪随机统计特性,这为信息隐藏发现性检测提供了方便,很多信息隐藏检测都是建立在密文伪随机分布的基础上. 我们提出一种本身具有抗破译能力的信息隐藏技术,密文隐藏前就无

需进行加密预处理. 这对信息隐藏提高抗发现检测能力无疑有积极意义.

4　抗取证信息隐藏系统安全性分析

抗取证安全性一般假设攻击者已知用户使用的信息隐藏技术,但不掌握用户每次信息隐藏通信的密钥. 根据这些先验知识,攻击携密载体,并取得证据性的数据,例如密文长度、隐藏密钥乃至密文原文. 因此可知,穷举密钥的代价反映了抗取证安全性.

以 *F*5 算法为例,不同的隐写编码代表不同的修改模式,大量的隐写编码对应大量互不相通的修改模式来保证算法空间的容量. *F*5 算法采用矩阵编码,矩阵编码可充分利用可携密数据位,在只做少量修改的前提下携带更多的秘密信息. 汉明纠错编码的码长等效于可携密数据的位数,要传递的信息位数等效于要携带的密文位数,纠错的位数等效于可修改的位数. 根据汉明编码理论我们很容易设计出$(2^k-1,k,1)$嵌入算法,以 $k=4$ 为例,即若采用(15,4,1)嵌入方法,即一个分组内的 15 个可用载体数据为 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{14})$,欲嵌入的秘密信息为 $\boldsymbol{S}=(s_0,\ s_1,\ s_2,s_3)$,并记

$$\boldsymbol{H}=\begin{pmatrix}1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\end{pmatrix}$$

计算 $\boldsymbol{Y}=\boldsymbol{H}\cdot\boldsymbol{X}$

如果 $\boldsymbol{Y}=\boldsymbol{S}$,则不需做任何修改. 如果不等,计算 $\boldsymbol{Y}-\boldsymbol{S}$,修改对应的列. 秘密数据提取非常简单,直接将矩阵 $\boldsymbol{H}$ 与可用载体数据相乘即可.

通过任意交换嵌入矩阵的两列,就可以形成一个新的嵌入矩阵. 不同的嵌入矩阵有 15! = 1307674368000 种. 不同的矩阵对载体实施的修改不同,因此可以说有 15! 种不同的嵌入算法. 这样一来,嵌入矩阵和密码算法中的密钥非常相似,通过修改嵌入矩阵就可以控制嵌入算法.

通过以上实验和分析我们可以看出,在第三部分提出的抗取证信息隐藏模型,不仅可以保证信息隐藏的不可感知性,还能保证在信息隐藏技术被攻击者掌握的情况下,用户轻易不会被穷举密钥攻击和取证.

5　结论和展望

本文在总结近几十年来信息隐藏对抗中发展成果的基础上,针对信息隐藏研究停留在实验室脱离实际的现状,提出抗取证信息隐藏框架,从理论上建立多模态信息隐藏通信的数学模型. 在该模型中体现信息隐藏盲检测和取证检测两种攻击方式,体现用户通过密钥对信息隐藏的参与性. 经理论分析和初步的实验验证,抗取证信息隐藏框架可以增强信息隐藏技术的安全性和实用性.

未来,大数据时代必然引起互联网内容的爆炸式增长. 在这种情况下,一方面我们可以预见,社会需求的推动,无疑会推进信息隐藏技术的普及应用,抗取证信息隐藏可以让信息隐藏技术走出实验室,飞入寻常百姓家;另一方面,抗取证信息隐藏模型不仅会为普通大众提供新的通信保护手段,更重要的是它会为信息隐藏开辟一个新的研究分支. 不再让信息隐藏研究只是纠结于在哪儿改、怎样改,藏得好,检测技术不再纠结于如何增加分类特征、提高分类器性能,才能提高检测指标,为大数据时代信息隐藏领域的研究人员提供一条新的研究思路,即如何更加全面、更加深入和更加实用地研究信息隐藏技术.

参考文献

[1] 钮心忻. 信息隐藏与数字水印[M]. 北京:北京邮电大学出版社,2004.

[2] 陈波,谭运猛,吴世忠. 信息隐藏技术综述[J]. 计算机与数字工程,2005,2:21 - 23.
Chen B,Tan Y M,Wu S Z. Research on information hiding techniques[J]. Computer and Mathematical Engineering,2005,2:21 - 23. (in Chinese)

[3] 张茹,杨榆. 数字版权管理[M]. 北京:北京邮电大学出版社,2008.

[4] C Cachin. An information-theoretic model for steganography[J]. Information and Computation,2004,192(1):41 - 56.

[5] T Pevny,J Fridrich. Benchmarking for steganography[A]. Proceedings of the 10th Information Hiding Workshop[C]. Santa Barbara, CA, USA: Springer-LNCS, 2008. 5284:251 - 267.

[6] A D Ker. Estimating steganographic fisher information in real images[A]. Proceedings of the 11th Information Hiding Workshop[C]. Darmstadt, Germany: Springer-LNCS, 2009. 5806:73 - 88.

[7] T Filler,J Fridrich. Fisher information determines capacity of secure steganography[A]. Proceedings of the 11th Information Hiding Workshop[C]. Darmstadt: Springer-LNCS, 2009. 5806:31 - 47.

[8] A D Ker. A capacity result for batch steganography[J]. IEEE Signal Processing Letters,2007,14(8):525 - 528.

[9] A D Ker,T Pevny,J Kodovsky,J Fridrich. The square root law of steganographic capacity[A]. Proceedings of the 10th ACM Multimedia and Security Workshop (MM & Sec)[C]. Oxford,UK:2008. 107 - 116.

[10] T Filler,A D Ker,J Fridrich. The square root law of steganographic capacity for markov covers[J]. Security,Steg-

anography, and Watermarking of Multimedia Contents XI, Proceedings of SPIE, 2009, 7254: 18 – 22.

[11] 王朔中,张新鹏,张开文等. 数字密写与密写分析[M]. 北京:清华大学出版社,2005.

[12] J. Fridrich. Steganography in digital Media: Principles, Algorithms, and Applications [M]. Cambridge: Cambridge University Press, 2010.

[13] 张涛,平西建. 空域 LSB 信息伪装的隐写分析及其对策[J]. 通信学报,2003,24(12):156 – 163.
Zhang T, Ping X J. Steganalysis of spatial LSB-based steganagraphic algorithms and countermeasures[J]. Journal of China Institute of Communications, 2003. 24(12): 156 – 163. (in Chinese)

[14] Solanki K, Sarkar A, Manjunath B S. YASS: yet another steganagraphic scheme that resists blind steganalysis[A]. Information Hiding, 9th International Workshop[C]. Saint Mala, France: Springer-Verlag, 2007. 16 – 31.

[15] Luo W Q, Huang F J, Huang J W. A more secure steganagraphy based on adaptive pixel-value differencing scheme [J]. Multimedia Tools and Applications, 2011, 52(2): 404 – 430.

[16] P Sallee. Model-based steganography[A]. Digital Watermarking, 2nd International Workshop [C]. New York: Springer-Verlag Press, 2004. 154 – 167.

[17] P Sallee. Model-based methods for steganography and steganalysis [J]. International Journal of Image and Graphics, 2005, 5(1): 167 – 190.

[18] Amin P K, Liu N, Subbalakshmi K P. Statistically secure digital image data hiding [J]. IEEE Multimedia Signal Processing, 2005: 497 – 500.

[19] Sarkar A, S K, Mdahow U. Secure steganagraphy: statistical restoration of the second ordor dependencies for improved security[J]. Acoustics, Speech and Signal Processing, 2007: 277 – 280.

[20] 张石树,汤光明. 一种保持频域高阶统计特性不变的隐写算法[J]. 计算机工程,2008,34(17):149 – 153.
Zhang S S, Tang G M. Steganograph algorithm on preservation of high order statistics in frequency domain[J]. Comupter Engineering, 2008. 34(17): 149 – 153. (in Chinese)

[21] A D Ker. Perturbation hiding and the batch steganography problem[A]. Proceedings of the 10th International Workshop on Information Hiding [C]. Santa Barbara, CA, USA: Springer-LNCS, 2008. 5284: 45 – 59.

[22] Tang WX, Li B, Luo WQ , Huang JW. Clustering steganographic modification directions for color components[J]. IEEE Signal Processing Letters, 2016, 23(2): 197 – 201.

[23] K. Petrowski. Psteg: steganographic embedding through patching[A]. Proceedings of the 30th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)[C]. Philadelphia, 2005. 537 – 540.

[24] Wu K C, Wang C M. Steganography using reversible texture synthesis[J]. IEEE Transactions Image Processing, 2015, 24(1): 130 – 139.

[25] 孙星明,殷建平,陈火旺等. 汉字的数学表达式研究[J]. 计算机研究与发展,2002,39(6):707 – 711.
Sun X M, Yin J P, Chen H W, et al. On mathematical expression of a Chinese character[J]. Journal of Computer Research and Development, 2002, 39(6): 707 – 711. (in Chinese)

[26] Z Zhou, H. Sun, R Harit, X Sun, X Chen. Coverless image steganography without embedding [J]. LNCS, 2016, 9483: 123 – 132.

[27] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images [J]. Magazine of IEEE Multimedia, Special Issue on Security, 2001, 22 – 28.

[28] C Yang, X Luo, F Liu. Embedding ratio estimating for each bit plane of image[A]. Proceedings of the 11th Information Hiding Workshop [C]. Darmstadt, Germany: Springer-LNCS, 2009. 5806. 59 – 72.

[29] A D Ker. Derivation of error distribution in least squares steganalysis[J]. IEEE Trans Information Forensics and Security, 2007, 2(2): 140 – 148.

[30] Fridrich J, Goljan M, Hogea. Steganalysis of JPEG: breaking the F5 algorithm[A]. Proceedings of the 5th Information Hiding Workshop [C]. The Netherlands: Springer-LNCS, 2002. 2578: 310 – 323.

[31] X Luo, D Wang, P Wang, F Liu. A review on blind detection for image steganography [J]. Signal Processing, 2008, 88: 2138 – 2157.

[32] I Avcibas, M Kharrazi, N D Memon, B. Sankur. Image steganalysis with binary Similarity measures [J]. EURASIP Journal on Applied Signal Processing, 2005, 17: 2749 – 2757.

[33] T. Pevny and J. Fridrich. Merging markov and DCT features for multi-class JPEG steganalysis[J]. Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, Proceedings of SPIE, 2007, 6505: 3 – 4.

[34] Y Q Shi, C Chen, W Chen. A Markov process based approach to effective attacking JPEG steganography [A]. Proceedings of the 8th Information Hiding Workshop [C]. Alexandria, VA, USA: Springer-LNCS, 2006. 4437: 249 – 264.

[35] X Y Luo, F L Liu, S G Lian, C F Yang, S Gritzalis. On the typical statistic features for image blind steganalysis [J]. IEEE Journal of Selected Areas in Communications, 2007, 29(7): 1404 – 1422.

[36] T Penvy, P. Bas, J Fridrich. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Trans Information Forensics and Security, 2010, 5(2): 215 – 224.

[37] Han Zong, Fenlin Liu, Xiangyang Luo. A wavelet-based blind JPEG image steganalysis using co-occurrence matrix [A]. The 11th International Conference on Advanced Communication Technology[C]. Phoenix Park, Republic of Korea, 2009. 1933 – 1936.

[38] Y Wang, J Liu, W Zhang. Blind JPEG steganalysis based on correlations of DCT coefficients in multi-directions and calibrations[A]. Multimedia Information Networking and Security, International Conference[C]. Hubei, 2009. 495 – 499.

[39] W Lie, G Lin. A feature-based classification technique for blind image steganalysis[J]. IEEE Trans Multimedia, 2005, 7(5): 1007 – 1020.

[40] T Pevny, J Fridrich. Novelty detection in blind steganalysis[A]. Proceedings of the 10th ACM Multimedia and Security Workshop (MM & Sec)[C]. Oxford, UK: 2008. 167 – 176.

[41] J Fridrich, J Kodovsky. Rich models for steganalysis of digital images[J]. IEEE Trans Information Forensics and Security, 2012, 7(3): 868 – 882.

[42] B Chen, G Feng, X Zhang, F Li. Mixing high-dimensional features for JPEG steganalysis with ensemble classifier [J]. Signal, Image and Video Processing, 2014, 8(8): 1475? 1482.

[43] F Li, X Zhang, B Chen, G Feng. JPEG steganalysis with high-dimensional deatures and bayesian ensemble classifier[J]. IEEE Signal Processing Letters, 2013, 20(3): 233 – 236.

[44] 王丽娜,王旻杰,邵锋,翟黎明,任延珍. 面向隐写分析的数字图像固有特性研究[A]. 第十一届全国信息隐藏暨多媒体信息安全学术大会[C]. 西安, 2013. 336 – 344.
Wang L N, Wang M J, Shao F, Zhai L M, Ren Y Z. Research of image properties for steganalysis[A]. Proceedings of of 11th China Information Hiding Workshop[C]. Xi'an, China, 2013 336 – 344. (in Chinese)

[45] A Ker, T Pevny. Identifying a steganographer in realistic and heterogeneous data sets[J]. Media Watermarking, Security, and Forensics, Proceedings of SPIE, 2012: 8303.

[46] 周琳娜,等. 数字图像内容取证[M]. 北京:高等教育出版社, 2011. .

[47] Crandall r. Some Notes on Steganography[EB/OL]. http://os. inf. tudresden. de/ ~ westfeld/ randall. pdf, 2007. 12.

[48] 李玉辉,刘九芬,张卫明. 基于二元 golay 隐写码的快速隐写算法[J]. 信息工程大学学报, 2007, 8(3): 269 – 271.
Li Y H, Liu J F, Zhang W M. Fast steganographic algorithm based on the golay codes[J]. Journal of Infromation Engineering University, 2007, 8(3): 269 – 271. (in Chinese)

[49] Schonfeld D, Winlker A. Embedding with syndrome coding based on BCH codes[A]. Proceedings of the 8th ACM multimedia and security workshop[C]. Geneva, Switzerland, 2006. 214 – 223.

[50] X Zhang, S Wang. Dynamical running coding in digital steganography[J]. IEEE Signal Processing Letters, 2006, 13(3): 165 – 168.

[51] F Willems, M Dijk. Capacity and codes for embedding information in gray-scale signals[J]. IEEE Trans Information Theory, 2005, 51(3): 1209 – 1214.

[52] J Fridrich, T Filler. Practical methods for minimizing embedding impact in steganography[J]. Electronic Imaging, Media Forensics, and Security IX, Proceedings of SPIE, 2007, 6050: 1 – 15.

[53] J Fridrich, M Goljan, P Lisonek, D Soukal. Writing on wet paper[J]. IEEE Trans Signal Processing, 2005, 53(10): 3923 – 3935.

[54] W Zhang, X Zhang, S Wang. Maximizing steganagraphic embedding efficiency by combining Hamming codes and wet paper codes, [A]. Proceedings of the 10th International Workshop on Information Hiding[C]. Santa Barbara, CA, USA: Springer-LNCS, 2008. 5284: 60 – 71.

[55] T Filler, J Judas, J Fridrich. Minimizing additive distortion in steganography using Syndrome-Trellis code[J]. IEEE Trans Information Forensics and Security, 2011, 6(3): 920 – 935.

[56] T Pevny, T Filler, P Bas. Using high-dimensional image models to perform highly undetectable steganography [A]. Proceedings of the 12th Information Hiding Workshop[C]. Calgary, Canada: Springer-LNCS, 2010. 8948: 161 – 171.

[57] V Holub, J Fridrich. Designing steganagraphic distortion using directional filters[A]. Proceedings of the 4th IEEE International Workshop on Information Forensics and Security (WIFS)[C]. Tenerife, Spain: 2012. 234 – 239.

[58] V Holub, J Fridrich. Digital image steganography using universal distortion[A]. Proceedings of the 1st IEEE Information Hiding and Multimedia Security Workshop (IH& MMSec)[C]. Montpellier, France: 2013. 59 – 68.

[59] B Li, S Tan, M Wang, J Huang. Investigation on cost assignment in spatial image steganography[J]. IEEE Trans. Information Forensics and Security, 2014, 9(8): 1264 – 1277.

[60] B Li, M Wang, J Huang, X Li. A new cost function for

spatial image steganography[A]. Proceedings of the 21th IEEE International Conference on Image Processing (ICIP)[C]. Paris, France: 2014. 4206 – 4210.

[61] J Fridrich, J Kodovsky. Multivariate Gaussian model for designing additive distortion for steganography[A]. Proceedings of the 38th IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)[C]. Vancouver, BC, Canada: 2013. 2949 – 2953.

作者简介

黄殿中 男,1952 年生于江苏新沂,中国通用技术研究院研究员. 主要研究方向为信息安全、信号处理与数字水印等.

张静飞(通信作者) 女,1981 年生于河南南阳,中国通用技术研究院副研究员. 研究方向为数字图像处理、多媒体信息安全.
E-mail: buptzhjf@163.com

张 茹 女,1976 年生于山东济南,北京邮电大学网络空间安全学院副教授. 研究方向为数字内容安全、应用密码学、信息隐藏等.

李鹏超 男,1983 年生于河北承德,北京电子技术应用研究所助理研究员. 研究方向为信号处理、多媒体信息安全.

郭云彪 男,1969 年生于河北赵县,北京电子技术应用研究所研究员,中国电子学会高级会员,中国计算机学会高级会员. 主要研究方向为信号处理、多媒体信息安全.