电子虚拟空间的信息犯罪分层研究

周 健[1,2],孙丽艳[1]
(1. 安徽财经大学 管理科学与工程学院,安徽 蚌埠 233041;
2. 北京邮电大学 计算机学院,北京 100083)

摘 要:具有非暴力、强隐蔽性和跨时空特点的信息犯罪难于跟踪取证,容易造成信息犯罪的蔓延和不可控性。针对电子虚拟环境中的信息犯罪取证问题,在分析虚拟环境电子证据的内容和表现形式的基础上,提出了基于虚拟环境的犯罪行为层次和特点的电子证据数据链。该数据链将犯罪行为所经过的物理层、网络层、操作系统层、应用层和表示层作为现实虚拟链、物理技术链、数据链和软件工具链,将犯罪证据在每个层次的遗留痕迹形成一个完整逻辑的犯罪证据链。电子证据数据链不仅能够为信息犯罪提供更为完整的证据,有效提高了强隐蔽性和跨时空虚拟环境中犯罪证据的可追溯性,而且加强了犯罪数据保护,可为在虚拟和现实空间的犯罪证据提供连接桥梁,为在分层的虚拟空间中犯罪行为的研究提供新方法。

关键词:信息犯罪;信息犯罪层次;电子证据;电子虚拟环境
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2017)08-0125-05
doi:10.3969/j.issn.1673-629X.2017.08.026

Investigation on Stratification of Information Crime in Electronic Virtual Environment

ZHOU Jian[1,2], SUN Li-yan[1]
(1. School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu 233041, China;
2. School of Computer, Beijing University of Posts and Telecommunications, Beijing 100083, China)

Abstract: Information crime has characteristics including non-violence, high covert and across space and time so that the evidence is difficult to acquire and track due to the uncontrollable spread in information crime. To deal with the question of achieving information crime proof in electronic virtual environment, on the basis of analyzing the content and form of information crime proof in electronic virtual environment, the chain of electronic proof based on layer and characters of crime in virtual environment has been presented. Furthermore the virtual chain, physical technology chain, data link and software tool chain have been formed when the crime behavior happens in the physical layer, network layer, operating system layer, application layer and presentation layer. The chain of electronic proof in the electronic virtual environment layer has been constructed, which not only provides the more comprehensive proof for information crime to improve the traceability of evidence in strong concealment and train-time-space electronic virtual environment, but also strengthens the protection of data on information crime, and the traces of crime have been left behind in every level for the emerging of complete criminal evidence. Therefore the chain has built the bridge between the virtual and the reality on information crime. Investigations on electronic virtual environment layer have provided new method for studies on information crime.

Key words: information crime; information crime level; electronic proof; electronic virtual environment

0 引 言

伴随信息技术的发展,信息犯罪[1-3]作为一种日渐独立的犯罪形态登上历史舞台,引起了高度关注。它具有丰富的内涵,是一种非常复杂的社会行为和现象[4-5]。信息技术的触角几乎涉及所有行业,这也导致信息犯罪覆盖了社会的各个层面[6]。自从 1958 年

收稿日期:2016-04-18 **修回日期**:2016-08-03 **网络出版时间**:2017-06-05
基金项目:国家自然科学基金资助项目(61402001);安徽省高校自然科学研究项目(KJ2013B001);安徽财经大学校级重点科研课题(ACKY1517ZDB))
作者简介:周 健(1979-),男,博士,副教授,博士后,CCF 会员,研究方向为密钥管理、无线网络安全、深空网络。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20170605.1506.008.html

在美国发生第一起计算机犯罪起,从棱镜门的国家间的信息对抗、苹果和 FBI 的国家与公司的保密技术争端,到个人信息泄露、污染、盗用等等[7],利用信息技术的犯罪行为大幅上升,且每年以 10% ~15% 的速率增长。保护信息安全成为国家安全的重要内容[8],习近平在中央网络安全和信息化领导小组第一次会议中强调:“没有网络安全就没有国家安全。”在这种背景下,深入研究信息犯罪的相关问题,无疑是十分必要的。然而信息犯罪与其他形式的犯罪有着显著的区别,尤其信息犯罪借助电子虚拟环境,具有其独特的社会行为特点和技术特点[9-10],因此,深入研究电子虚拟环境中信息犯罪的分层种类、电子证据、数据链具有重要意义。针对虚拟环境中的电子取证问题,对虚拟环境进行了分层,并根据层次建立了信息犯罪的数据链,因而可以构建完整、有效、可循的电子证据。

1 信息犯罪的定义和特点

信息科学的开放性、虚拟性、随机性、智能性、扩散性、高传输等特点[11]使得信息犯罪具有高智能、强隐蔽、时空跨越、多样性、非暴力性、低风险、非接触性和复杂性等特点[12-13]。

高智能:体现在高知识的犯罪人和高技术的软件工具。早期信息犯罪中,犯罪分子一般具有较高的文化程度,受过信息化专业技能训练,具有足够的专业知识和技能,针对特定的某一种数据,能够熟练使用信息化工具。随着信息化技术的普及,各种信息工具的不断涌现,一般技术者可以充分利用多种信息工具的组合实施信息犯罪,例如盗号软件破解密码实施金融诈骗,信息犯罪具有从高学历人群扩散到一般学历人群的趋势。

强隐蔽:行为人良好的教育背景和高智商具有很强的欺骗性,信息犯罪隐藏于虚拟环境中,分层次的透明体系结构也决定顶层的用户无法感知底层的数据运行状况。以二进制代码为数据形式的信息系统和信息数据可视化程度较低,数据的使用和实体世界的物品使用具有很大差别,实体世界的物品难于复制,使用中往往留下痕迹,难于销毁,虚拟世界的数据可以不留痕迹地使用、复制和删除。

时空跨越:在传统犯罪中,时间和空间往往占有重要的位置,而信息犯罪侵害过程充分利用信息技术的自动化、智能化,是超越时空的犯罪。信息犯罪往往是通过网络实施的,而互联网的覆盖范围十分广泛,行为人有条件也有时间在网络上寻找适合自己的作案目标,一段恶意代码可以被多重复制,往往并发侵害多个目标。

复杂性:体现在涉及范围和多种知识交叉。首先,信息网络开放性消除了家庭、社会以及国境线的界限;其次,信息技术已经完全融入现今社会的所有部门,信息犯罪往往是涉及多种行业技术的交叉犯罪,庞大的数据量和多种数据表现形式增加了犯罪行为分析的难度;最后,信息犯罪行为很容易在开放的环境中随机扩散,时间、地点的随意性和开放性,导致受害目标的不确定性和随机性。

非暴力倾向:信息犯罪很少涉及暴力冲突,一般没有直接的人员伤害和对个人利益造成的直接损失。一方面信息犯罪斗智不斗勇,犯罪者在生理、心理条件与暴力犯罪的犯罪者具有显著差异,犯罪人和受害者非直接接触,作案工具也由软硬件技术代替伤害性工具,电子虚拟环境中的数据成为犯罪者和被害者之间的工具、媒介和攻击对象,难以造成视觉冲击;数据侵害的危害效果具有延时性和隐蔽性,因此信息犯罪较少展现暴力,往往给公众一种欺骗性,直观印象造成公众的警惕性不高。

短时间和低成本:信息犯罪作案时间一般较短,且大多不需要犯罪分子亲临现场承担暴力风险,因此犯罪分子在作案时自我谴责和“现场”心理恐惧感大大降低,同时增加了犯罪行为的安全系数。被发现概率低、收集证据难、大多数受害者不愿报案致使信息犯罪案件的侦破难度大而且侦破率相对较低,例如美国第一起计算机犯罪直到 1966 年才被发现。信息犯罪具有高收益性,据美国斯坦福研究所统计,美国平均一起计算机犯罪案,罪犯获利 45 万美元,是常规犯罪案件的几十倍。

这些特点造成信息犯罪不易掌握犯罪证据和确定罪与非罪的界限等特点,加之信息化建设的总体安全性较低,重效益、轻安全,边设计边投入使用、缺乏规范的系统管理,以及法律不健全,各国制定的信息犯罪法律法规各不相同,而电子虚拟环境又不像国土具有明确的界线,造成信息犯罪的国际化发展,给立法带来了相应的困难,导致破案率和定罪率较低。在美国信息犯罪破案率不到 10% ,定罪不到 3% 。

目前学术界对信息犯罪的定义为“在信息活动的过程中,利用和针对信息而发生的犯罪现象就是信息犯罪,主要包括行为人以信息资源为侵害对象的犯罪和以信息科技为犯罪手段的犯罪两种类型”。从实体概念出发的信息犯罪定义强调信息技术的资源性和手段性,以及对现实社会的危害性,然而信息犯罪具有特定的活动空间电子虚拟环境,以计算机和网络限制电子虚拟环境过于狭隘,犯罪的实施主体可能是行为人和智能体的混合体。相对于普通犯罪,信息犯罪有特定的空间,即计算机和计算机网络的虚拟空间,因此信息犯罪应定义为:在电子虚拟空间中,利用电子虚拟空

间技术和针对电子虚拟空间资源而发生的犯罪现象,主要包括行为人、智能体或前两者混合体以电子虚拟空间资源为侵害对象的犯罪和以电子虚拟空间技术为犯罪手段的犯罪两种类型。

2　电子虚拟环境的犯罪行为分类

信息犯罪行为符合信息运动规律,研究信息犯罪在电子虚拟环境中的规律和特点有利于信息犯罪的分析与破案[14]。信息化规律的内涵包括五个方面:一是用于收集、加工、处理、输送、发布各类信息所需的硬环境,典型技术包括传感技术、通信技术和计算机技术;二是有一套完整的信息标准和科学的信息法规;三是有一套有效的经济信息化的应用系统;四是有多方面反映国民经济运行情况的各类数据库;五是有符合要求的高素质的人力资源。电子虚拟环境具有典型的分层特点,对信息犯罪的分层,有利于对信息犯罪进行分析,掌握犯罪人的生理和心理特点,进而掌握犯罪人对数据的管控能力,从而有利于案件的侦破。

物理层犯罪行为:处于信息犯罪的最底层,涉及传感、通信和计算机技术,只有特定的人群才具有实施的行为能力,犯罪人具有专业知识和系统处理数据的能力,以特定硬件设备资源为工具或攻击目标,包括损坏信息传输设备、降低信息设备效率、获取权限,受害者应对此类犯罪行为能力弱且隐蔽性强,具有很强的危害性。如使用汇编语言编写的系统级计算机病毒、无线信道密码破解等。

网络层犯罪行为:涉及通信和计算机技术,以网络资源为攻击目标,犯罪人具有专业知识和系统处理数据的能力,改变传输路径,破坏信道传输质量和环境的信息犯罪,受害者物理分布广泛,危害性强,具有专业知识的人群具有实施的行为能力,如借助互联网的各种网络数据窃取,数据流失控等。

操作系统层犯罪行为:涉及计算机软硬件技术,通过伪造身份获取非法控制某一系统权利的信息犯罪,如身份欺诈,犯罪人摧毁或制约他人的信息系统、数据库,具有专业知识的人群具有实施的行为能力,受害者是使用某一特定系统的特定人群。如军事系统入侵、金融财务系统入侵等。

应用层犯罪行为:涉及计算机软件技术,破坏或改变应用软件功能为目标的信息犯罪,犯罪人熟悉特定的系列软件工具,受害者使用的软件具有缺陷,各种植入式木马、利用计算机资源盗窃。

表示层犯罪行为:涉及计算机软件技术,犯罪人使用特定的软件工具作为盈利或损害他人利益,以获取各种信息为目的或借助信息技术获利的犯罪,如各种淫秽制品的散布,危害公共安全的谣言发布,信息污染、知识产权的破坏、个人信息盗取等。

信息犯罪行为的层次见图 1。

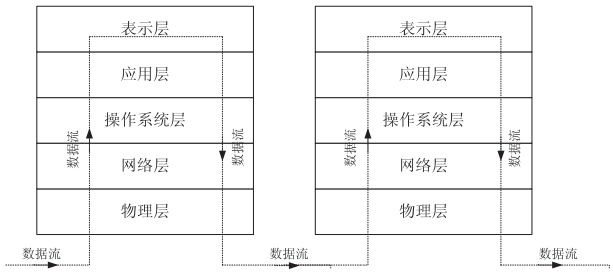

图 1　信息犯罪行为的层次

数据的分层和栈处理形式,决定了越靠近底层的信息犯罪行为危害性更大,隐藏性更深,也更不容易侦破。每个层次的犯罪也蕴含信息化五个方面的内容,物理层犯罪行为、网络层犯罪行为和操作系统层犯罪行为可以归结为高层次犯罪,具有物理层犯罪能力的行为人也必然具有发起高层信息犯罪的能力,反之则不然。物理层、网络层和操作系统层侧重信息资源破坏,而应用层和表示层侧重使用信息技术手段进行犯罪行为。

信息犯罪各层次特点见表 1。

表 1　信息犯罪各层次特点

犯罪层次	智能	隐蔽	随机性	潜伏性	管控数据	可视性
物理层	高	强	高	高	高	差
网络层	高	强	高	高	高	差
操作系统层	中	强	高	高	高	一般
应用层	低	低	低	低	低	强
表示层	低	低	低	低	低	强

信息犯罪的层次行为特征见表 2。

表 2　信息犯罪的层次行为特征

犯罪层次	行为目标	软硬件设备	专业知识
物理层	信息资源破坏	具体硬件	信息专业
网络层	信息资源破坏	具体硬件	信息专业
操作系统层	信息资源破坏	系统软件	混合专业
应用层	利用信息资源	应用软件	混合一般技能
表示层	利用信息资源	应用软件	混合一般技能

3　虚拟环境的犯罪数据链

电子虚拟环境中的资源和工具都是数据,信息运动规律在数据基础上,因此研究信息犯罪就必须重视电子虚拟环境中的数据,以及数据在动态环境中构建的数据链,完整的数据链将为犯罪行为提供必要的证明。

信息犯罪形成的数据链包括:

(1)现实虚拟链。如图 2 所示,电子虚拟环境建立在现实世界基础上,信息犯罪建立在电子虚拟环境

基础上,信息犯罪通过电子虚拟环境构建现实世界的联系必然会在电子虚拟环境和现实世界留下痕迹,因此信息犯罪存在实体->虚拟->实体的数据证据链路。同时,信息犯罪往往伴随其他犯罪行为,尤其在应用层和表示层信息犯罪中,由于信息犯罪处于纽带和催化地位,成为连接犯罪行为中重要的一环,构建虚拟现实的电子证据链尤为必要。

(2)物理技术链。软件建立在一定的硬件基础上,完全摆脱硬件设施的信息犯罪是不可能的,因此首先重视信息犯罪的硬件将为信息犯罪的侦破提供一个非常必要的前提条件。以传感技术、通信技术和计算机技术构成电子虚拟环境,三种技术都需要特定的硬件基础和规范,形成数据链,如监控摄像获取影像信息,窃听器获取音频信息;网络技术获取个人社交信息;利用数据挖掘技术进行数据分析和处理。

(3)数据链。信息犯罪本质上仍是一种信息活动,则其必然遵守信息科学的一般规律,具有信息的产生、提取、变换、检测、传递、存贮、识别和处理,包括寻求利用信息实现最优系统的途径,在数据处理上形成数据链。信息犯罪在犯罪实施过程中形成一个数据链,包括数据终端、数据传输、数据处理、数据库、数据仓库、数据使用。数据在数据链中的处理、转发、存储和分析都会为犯罪行为留下痕迹。

(4)软件工具链。目前的信息犯罪,并非像过去自己开发一段代码进行犯罪活动,很多信息犯罪首先借助各种软件工具,而且组合式使用,这些工具有特定的应用环境,能够为犯罪行为提供证明。

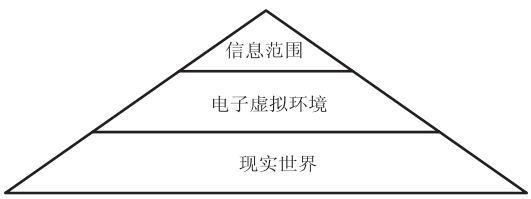

图 2 信息犯罪与电子虚拟环境、现实世界的关系

4 虚拟环境的电子证据

国内司法的指导思想是以事实为依据,以法律为准绳,打击计算机信息犯罪,法律依据就是对事实的证明,事实证明离不开证据。《中华人民共和国电子签名法》的第三条和第七条规定了电子证据的有效性和不可歧视性,电子证据作为八大证据类型之一[15]。计算机信息犯罪的特殊性在于,其一般不会在现实世界中留下一些传统意义上的证据,如物证、书证等,其证据一般是在计算机或网络的电子虚拟世界里,以电子证据的形式存在。因此,为了打击这类犯罪,必须研究电子证据的应用。电子证据的提取应遵循以下原则:确定电子证据的存储形式、位置、格式、附属文件或包头;不得损害目标设备中电子数据的完整性、真实性;电子证据与物理载体的无关性;不得将提取、生成的数据存储在原存储设备中;不得在原存储设备中安装新的程序;详细记录在线分析和提取的过程。

电子证据是指能够证明案件相关事实的电子数据文件,属于电子数据,遵从信息科学规律,在冯诺依曼结构计算机中,明确将存储列为核心,所有的数据处理、数据传输都以存储器为中心,在网络技术中,分组传输和数据封装成为一个基础。因此,电子证据具有三个特征:二进制为基础的数字化存在形式;不固定依附特定的载体;可以多次原样复制。这也导致电子证据与传统证据体系的部分规则存在矛盾,如最佳证据原则(只能采用的证据应该是最具证明力和说服力的证据形式,即证据原件,电子证据显然不符合)、非法证据排除等。同时,由于电子信息的动态性,它分为静态电子证据和动态电子证据。静态电子证据是指保存在非易失存储设备中的电子证据不会因外部环境变化(如断电)而丢失数据,如硬盘中的电子证据;动态电子证据是指网络传输、易失存储设备中的电子证据,当外界环境发生变化,其数据易发生变化,如内存中的电子证据。最后,电子证据的内容分为内容信息电子证据和附属信息电子证据。内容电子证据是指记载一定社会活动内容的电子证据,也是证据的正文;附属信息电子证据是指记录内容信息电子证据的形成、处理、存储、传输、输出等与内容信息电子证据相关的环境和适用条件等附属信息的证据。由于数据包采用分组传输和封装形式,因此某一层次的数据包的下一层次的数据报头是该数据包的附属信息电子证据。电子证据在信息犯罪的层次内容不同,物理层电子证据包括二进制文件、电磁信号等;网络层电子证据包括电子日志、网络地址、控制信令、数据包、网络协议等;系统层电子证据包括数据库文件、高级程序文件、电子日志、超文本等;应用层电子证据包括字处理软件、图形图像处理软件、视频音频处理软件、格式等;表示层电子证据包括字处理文件、图形图像文件、视频音频文件、电子虚拟物品等。

5 信息犯罪的数据保护手段

数据在信息化中处于核心地位,电子证据的保护属于数据保护,因此信息犯罪的防治也应将数据保护摆在一个核心位置。信息犯罪的防治包括技术、法律、伦理等手段,这里着重论述技术手段。在技术层面上,根据信息犯罪的层次特征采取应对措施:

(1)构建面向打击信息犯罪的网络安全架构,如火车票和无线通信卡的实名制购买。

(2)重视现代新型信息保密技术的开发利用,既

能“对症下药”,又是长远之计。信息保密技术包括人工智能与专家系统、信息资源保密技术、信息对抗技术、反动态跟踪技术、计算机系统安全技术、密码技术和密码分析技术、数据库安全技术、软件加密技术、数据加密技术等。

(3)信息犯罪提供建立可视化技术,即利于对犯罪行为的直观认识,也利于信息犯罪的立案和侦破。

(4)进一步丰富数据管理和分析方法,只有让可记录、有限制的网络行为,信息平台终端对数据的操作行为具有限定性和可记录性。

(5)建立在信息技术层面上的网络行为的惩罚机制,如同刑事惩罚一样,当行为人利用网络实施非法行为时,通过限制、惩罚其网络行为,达到威慑力。

(6)建立不同层次的信息犯罪电子证据的获取方法,对电子证据的读写权限进行限制。

6　结束语

信息犯罪依托的电子虚拟环境与现实社会具有显著差别,尽早开展虚拟环境下的信息犯罪行为研究和技术保护有利于虚拟环境的秩序,通过对虚拟环境的分层,分析各层的犯罪行为,从而建立信息犯罪的数据链,有利于信息犯罪证据的收集、分析和保护。

参考文献:

[1] Choudhury R R, Basak S, Guha D. Cyber crimes-challenges & solutions[J]. International Journal of Computer Science and Information Technologies, 2013, 4(5): 729-732.

[2] 文　军. 信息社会信息犯罪与信息安全[J]. 电子科技大学学报:社会科学版, 2000, 2(1): 21-25.

[3] 朱晓征. 信息犯罪原因探析[J]. 法制与社会, 2015(23): 287-288.

[4] 徐澜波. 计算机信息犯罪研究[J]. 社会科学, 2004(4): 51-57.

[5] 马海群. 论信息犯罪及其控制[J]. 中国图书馆学报, 1996, 22(1): 41-43.

[6] Laybats C, Tredinnick L. Information security[J]. Business Information Review, 2016, 33(2): 76-80.

[7] Liu Lu. The study on invading personal information crime in criminal law[J]. Software Engineering and Knowledge Engineering: Theory and Practice, 2012(44): 927-934.

[8] Traunmueller M, Quattrone G, Capra L. Mining mobile phone data to investigate urban crime theories at scale[C]//International conference on social informatics. [s. l.]: Springer International Publishing, 2014: 396-411.

[9] 马进保. 高科技语境下的电子信息犯罪[J]. 中国人民公安大学学报:社会科学版, 2009(3): 152-157.

[10] 贺曙敏, 李锡海. 现代化与信息犯罪[J]. 山东大学学报:哲学社会科学版, 2010(4): 35-42.

[11] 李菊萍. 信息犯罪探析[J]. 安徽工业大学学报:社会科学版, 2002, 19(2): 63-64.

[12] 张　莉. 网络环境下我国信息犯罪的分析及对策研究[J]. 农业图书情报学刊, 2005, 17(7): 131-134.

[13] 高德胜, 马海群. 信息犯罪新论[J]. 求是学刊, 2006, 33(3): 92-96.

[14] 张　磊, 许慧敏. 电子证据在打击计算机信息犯罪中的应用研究-以《刑法修正案》(七)为契机[J]. 安徽警官职业学院学报, 2011, 10(1): 60-63.

[15] 常　怡, 王　健. 论电子证据的独立地位[J]. 法学论坛, 2004, 18(6): 66-74.

(上接第 124 页)

字水印算法[J]. 电子学报, 2006, 34(12): 2134-2137.

[4] Tataru R L, El Assad S, Deforges O. Improved blind DCT watermarking by using chaotic sequences[C]//International conference for internet technology & secured transactions. [s. l.]: IEEE, 2012: 46-50.

[5] Sridhar B, Arun C. On secure multiple image watermarking techniques using DWT[C]//3th IEEE international conference on computing communication & networking technologies. [s. l.]: IEEE, 2012: 1-4.

[6] Deb K, Sajib Al-Seraj M S, Hoque M M, et al. Combined DWT-DCT based digital watermarking technique for copyright protection[C]//Proceedings of the 7th IEEE international conference on electrical & computer engineering. Bangladesh: IEEE, 2012: 458-461.

[7] 孙秋冬, 马文新, 颜文英, 等. 数字图像的随机置乱加密及其与 Arnold 变换技术的比较[J]. 上海第二工业大学学报, 2008, 25(3): 159-163.

[8] 王　弼, 张　忠. 离散小波变换和混沌结合的数字图像水印算法[J]. 电子测量与仪器学报, 2008, 22(5): 16-20.

[9] 卢宗庆, 梅蕤蕤, 黄敬雄. 基于位平面的数字水印算法[J]. 计算机工程与应用, 2003, 39(6): 79-81.

[10] Guo C, Xu G, Niu X, et al. A color image watermarking algorithm resistant to printscan[C]//IEEE international conference on wireless communications, networking and information security. [s. l.]: IEEE, 2010: 518-521.

[11] 刘国贺, 李玉惠, 李　勃, 等. 基于 FPGA 的数字图像水印实时嵌入系统的设计与实现[J]. 电子技术应用, 2010(3): 27-30.

[12] 牛少彰, 舒南飞. 数字水印的安全性研究综述[J]. 东南大学学报:自然科学版, 2007, 37(S1): 220-224.

[13] 王树梅, 赵卫东, 王志成. 一种基于混沌变换的自适应盲水印[J]. 计算机仿真, 2007, 24(11): 129-133.

[14] 王万良, 管　秋, 杨旭东. 小波域数字图像水印改进算法及其性能分析[J]. 计算机辅助设计与图形学学报, 2004, 16(9): 1235-1239.