屏幕防窃拍方法综述

王晓媛 张文涛
(中国航天系统科学与工程研究院 北京 100037)

摘 要 如今,手机等设备的拍照性能愈发强大,其在给人们的生活带来便捷和快乐的同时,也为不法分子窃取企业商业秘密乃至国家秘密降低了犯罪成本,便捷而隐蔽的窃密方式给信息安全的防范工作带来了极大挑战。针对屏幕防窃拍方法,文中基于已有的相关学术研究和商业方案,介绍了 3 类屏幕防窃拍方法,分别为信息隐藏显示法、摄像头检测法和屏幕水印法,从信息安全防护角度分析了各类方法的特征、优势与限制。基于各类方法的局限性,最后提出了基于计算机视觉的新解决思路。

关键词 防窃拍方法,信息隐藏显示,摄像头检测,屏幕水印,计算机视觉
中图法分类号 TP30 **文献标识码** A

Overview of Preventing Candid Photos Methods for Electronic Screens

WANG Xiao-yuan ZHANG Wen-tao
(China Aerospace Academy of Systems Science and Engineering, Beijing 100037, China)

Abstract Nowadays, the performance of mobile phones and other devices has become more and more powerful. It brings convenience and entertainment to people's life. At the same time, it also reduces the cost of crime to steal business secrets even national secrets. The convenient and covert ways of stealing secrets have brought great challenges to information security. According to existing academic research and business solutions, this paper introduced three kinds of methods: hiding display information, detection camera and screen watermarking. Then it analyzed the characteristics, advantages and limitations of various methods from the angle of information security protection. Finally, a new solution based on computer vision was proposed to avoid the limitations.

Keywords Preventing candid photos methods, Hiding display information, Detection camera, Screen watermark, Computer vision

1 引言

信息网络的快速发展为企事业单位的日常办公及生产制造提供了极大的便捷,但随着窃密手段的不断升级[1],保护网络中重要信息的安全也成为越来越严峻的挑战。目前,全球数据泄密事件在逐年增加,泄密方式也在多样化,但从统计数据[2]可以看出,针对物理隔离或逻辑隔离网络的攻击手段未出现突破性的方式,尤其近几年从窃密代价的角度出发,窃密手段的重点从直接攻击网络向迂回策反内部人员方向转变。内部人员利用单位内部管理和技术上的漏洞,以偷盗硬盘、光盘刻录、U 盘转储[3]等方式进行窃密,但随着我国相关网络安全防护指南的推出和普及,以及各单位对内部保密管理的愈发重视,内部人员通过上述传统方式窃密的成本和难度越来越大。随着手机功能的不断强大,其拍照性能得到飞跃提升,内部人员使用手机直接拍摄屏幕内容变得简单易行,具有便携性和隐蔽性,且工作场合下携带手机已成习惯,更令人疏于防范[4]。另外,目前各单位针对手机对屏幕进行拍照的行为仅有管理制度,即禁止携带手机进入重要工作场所或明令禁止使用手机对屏幕进行拍摄,但制度落实过于依赖员工们的自觉性和相互监督,制度执行效果不佳,监管部门缺少相应的技术监管手段,无法做到无时无刻的监督,这也给不法分子带来了可趁之机,增大了拍摄泄密的风险。传统方法和手机拍摄屏幕方法的对比如表 1 所列。

近年来,通过对屏幕进行拍照窃取重要信息的案件时有发生,一旦重要信息泄漏,将对企业乃至国家带来巨大损失,因此针对新的应用需求,研究屏幕防窃拍的方法势在必行。本文从国内外研究现状入手,对现有可行方法进行分类,并针对每一种方法进行了分析,最后提出了一种新的方法。

表 1 两种窃密手段的对比情况

窃密手段	响应时间	难易程度	防护措施	可追溯性	隐蔽性	窃密的可能性
设备接入计算机	传递周期较长	技术支持及防追踪能力	已有数据接口防护产品	较强	较弱	较小
设备对屏幕拍照	快速获取,即刻传递	无技术要求	有制度规定,缺少技术手段	较弱	较强	较大

2 屏幕防窃拍方法概述

屏幕防窃拍,可以理解为在使用计算机处理重要信息时,防止显示器上的重要信息通过拍照、录像的方式被窃取的技术。一般来说,屏幕防窃拍可以在事件发生前进行威慑和预警,可以在事件发生时进行及时阻断,亦可以在事件发生后进

王晓媛(1993—),女,硕士生,主要研究方向为信息安全,E-mail:wxy13381216098@163.com;张文涛(1971—),男,硕士,研究员,主要研究方向为信息安全。

行有效审计并追溯以减少或控制损失,具有预防性、检测性、纠正性和威慑性。

目前,国外屏幕防窃拍的方法主要应用于电影版权保护和屏幕敏感信息保护等方面,根据不同的应用背景,主要采用两种方法:1)直接检测摄像头的物理特性,如光特性、无线通信特性(若采用无线传播)等,该方法直接了当,针对性强。2002 年,Roessler 汇总了检测摄像头的方法,提出了光检测和通信检测的方法[5];2005 年,Truong 等对摄像手机的大规模使用产生了担忧,因此提出了通过摄像头镜面反射光检测的方法[6]检测一定范围内正在拍摄的手机,即根据特定材质摄像头的反射高光,通过设置检测光源来主动侦查和定位摄像头。这种方法有监测范围不广等局限性,随后部分学者以及商业公司将其改造,使用红外线[7-10]进行检测,改善了其使用范围不广、使用环境苛刻、对正常使用者造成影响等问题,至此使用光检测的方法逐渐定型,这是目前使用比较广泛的方法;无线通信检测是针对无线摄像头的,其采用 Wifi 等检测设备来检测异常数据传输。2)在屏幕中隐写特殊识别信息,当有信息被摄像头拍摄外泄后能够进行事件追溯和追责。目前对屏幕水印的研究比较多,有学者利用此技术防止破坏物理隔离网络进行窃密[11],也有学者利用此技术解决电影版权问题,不断提高算法的鲁棒性,取得了较好的效果[12-13]。2014 年,Maciej 等首次提出将此技术应用于屏幕防窃拍中[14],以识别和追踪泄漏的数据。

近年来,我国信息安全产业发展迅猛,针对普遍、直观的传统安全威胁研发了很多的技术防护手段但针对非授权屏幕拍照等非传统意义上的安全威胁并未重视,针对此问题的国内学术研究和商业方案并不多见,但也在国外研究的基础上进行了一定的创新和发展。2013 年,耿振民等发明了一种反泄密的方法[15],通过技术手段使受控计算机的屏幕上仅显示光标附近的 N 个字符,可在一定程度上减少屏幕被窃拍从而泄漏敏感信息的风险,从解决问题的角度看,这是一种简单妥协的解决方案。在摄像头检测方面,张文豪等直击问题根本,于 2013 年设计了一种基于光反射检测的方式识别摄像头的方法[16],进而解决防盗拍问题;2017 年,浙江大学江嘉恒延续了张文豪等人的思路,提出了一种基于电磁检测的防拍摄监测技术[17-18],并首次将该技术应用于屏幕防窃拍问题上,通过检测摄像头特有的 VLF 频段的辐射特征,设计了一种可以在较远距离中检测到被隐藏的摄像头的设备,这类方法为屏幕防拍摄提供了一种有效的预警和检测方法。在屏幕隐写信息方面,我国学者研究实现了将信息隐写至屏幕中,通过拍摄分析将信息还原[19],这是信息传递的方法,也可将其应用在屏幕信息泄漏追踪的研究工作中。另外我国一些厂家分析了市场实际需求后开发了相关的产品,2017 年 IP-guard、联软科技[20-21]等研发了屏幕水印产品,为企业快速追溯通过拍摄泄漏的信息的来源提供有效依据,将计算机信息(IP 地址、时间、地点等)隐藏于水印信息中,后续通过提取水印获取信息。这类产品为屏幕防拍摄提供了一种可审计、可追溯的方法。2018 年,北信源公司在内网安全管理系统添加新功能,推出终端屏幕数据泄漏追踪方案,在桌面、屏幕、打印和应用软件中添加常驻、动态或密文等多种水印,常驻水印用于提高终端用户对数据的保护警觉性,动态水印实现对高危敏感数据进行警示,密文水印实现数据泄漏的追溯。

3 常见屏幕防窃拍方法的分析比较

基于上述分析,目前屏幕防窃拍的主要方法可以归纳为以下 3 类:信息隐藏显示法、摄像头检测法和屏幕水印法。各类方法是基于不同技术提出的解决思路,因此每类方法都具有其特征、优势和限制。本节将具体介绍各类方法的基本原理、优势、局限性以及适用背景等。

3.1 信息隐藏显示法

信息隐藏显示法即为避免显示器在大规模显示文档时泄漏重要信息,采取的技术措施是对显示信息进行隐藏。目前有两种方式,第一种是物理措施,在显示屏上粘贴防窥膜,阻止其他人员在其他角度非授权获取屏幕信息;另一种方法是技术措施,人员处理文档时,仅显示光标附近的有限字符,使非授权人员拍照时无法同时获取所有的信息,进而防止了屏幕信息泄漏。

3.1.1 方法的基本原理

1)物理措施:根据人眼的视觉特点,在集中精力时人眼视度约为 25°,通过在显示屏上粘贴偏光膜等,使屏幕可视范围缩小在可控范围内,限制用户只能在水平方向约 30°的范围内看到计算机屏幕上的信息,可有效阻止其他人员在其他角度非授权获取屏幕信息。

2)技术措施:使用计算机打开文档进行处理和阅读时,应用程序产生读文件进程,计算机内核建立与硬盘之间的映射,将文件缓存到内存中。利用这一原理,首先在受控机的客户端上配置安全策略,设置防止拍照的文档及可显示的字符数量(N);然后,在内存中建立安全区,当打开列表中的文档时,将需要显示的信息缓存在安全区中,当浏览处理重要信息时,仅显示光标位置之前的 N 个字符(N 可以随需要进行调整),其他区域的字符通过使用特定字符(如空格)代替或者设置成与背景一样的颜色来进行隐藏[15]。该方法的流程如图 1 所示。

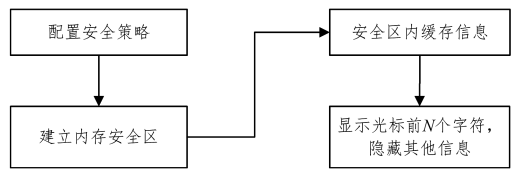

图 1 信息隐藏显示的基本流程

3.1.2 优势

物理措施可有效阻止不可视范围内任何光方式窃取信息的可能性。技术措施利用技术手段隐藏了屏幕显示的冗余信息,在一定程度上保护了信息的安全,同时降低了通过窃拍将信息泄漏的风险。

3.1.3 局限性

物理措施不可防止可视范围内的窃拍行为,也不可防止机器使用者违规拍摄的行为。

技术措施在满足防窃拍行为的同时,也带来了一定的局限性:1)摄像攻击局限,该方法可以避免窃拍的瞬时攻击,但对于长时间的摄像攻击的抵御能力不足;2)效率局限,在阅读文献时仅显示部分内容,对阅读的连续性有影响,工作效率可能会有影响;3)保护对象局限,该方法仅可应用于文本类型文件,图片、图纸等其他类型文件无法进行保护。

3.2 摄像头检测法

为达到屏幕防窃拍的目的,一种行之有效的方法是检测办公场所中的隐藏摄像头。摄像机一般由镜头和非线性元件

组成，其中非线性元件包括时钟电器、振荡器、电源开关、数字逻辑电路和处理器等。依据摄像头的组成部件与工作原理，衍生出多种摄像头检测方法，用来发现办公场中所有隐藏的用于窃拍的摄像头，并给出预警。

3.2.1　检测基本原理

摄像头本质上属于电子设备，依据电子设备工作的普遍特性和摄像头特有的结构与工作特点，衍生出一系列的屏幕防窃拍的摄像头检测方法。

1）基于镜头：所有的摄像头都需要镜头进行成像，大多数镜头为凸透镜，会发生物理折射。一种简单的方法是人工方法，在屋内处于黑暗状态下，使用白光进行扫射，若白光经过摄像机镜头，则会发生折射，呈现出彩色光线。另一种方法是仪器检测，基本原理如图 2 所示。仪器主要由光源模块、检测器和图像处理器 3 部分组成，在光源模块发出不可见光，当经过镜头回射光线至监测器，若出现高光现象，该高光交由图像处理器进行分析处理，若经算法处理高光为存在摄像头产生的，则产生警告[16]。

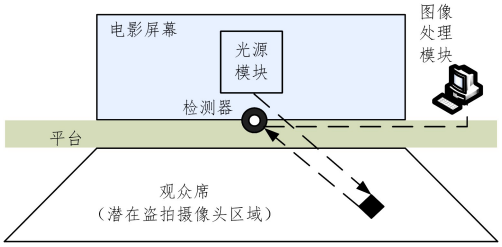

图 2　摄像头检测方法的硬件示意图[16]

2）基于电磁：摄像头成像依赖于时钟逐行逐像素扫描，时钟工作时会产生电磁泄漏，当屋内工作的电器关闭时，通过检测电磁便可以发现隐藏摄像头。分析摄像头的辐射特征发现，其总存在频率为 16kHz 左右的超长波甚低（ELF）频辐射[18]，因此可依靠辐射检测和计算机分析来检测摄像头是否存在。检测设备的基本结构如图 3 所示。

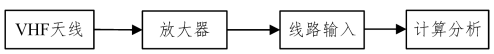

图 3　电磁检测设备基本结构

图 3 中，VHF 天线用于收集甚低频信号，放大器用于放大收集到的甚低频信号，计算机对收集到的信号进行分析，当频率信号出现明显波动时，认为发现工作的摄像头并产生报警行为。

3）基于热量：摄像头的图像传感器等部件工作时会散发热量，依据这一原理，利用热成像仪进行检测可以发现摄像头。

4）基于通信：摄像头采集到的视频信息需要进行传送，会存在有线或无线的数据传输口，射频扫描仪可以帮助检测屋内的通信出口，发现异常。

3.2.2　优势

现在主要的检测方法大都基于摄像头的物理特征，这些方法为屏幕防窃拍中检测摄像头的存在提供了解决思路。

基于镜头的检测方法适宜在光线较弱的条件下进行；基于电磁检测的方法可检测距离较远的隐藏摄像头，不受光线、温湿度等外界条件的影响，检测隐藏摄像头具有普适性。

3.2.3　局限性

基于镜头的方法对环境光线要求较高，不适用于在办公室环境中进行实时监测，不适于解决屏幕实时防拍照问题。

基于电磁的方法中，摄像头的电磁辐射通过加装电磁屏蔽设备，将弱化甚至消除电磁辐射信号，从而无法进行检测；办公环境下很多时候电磁信号较为复杂，尤其在生产现场，受到这些信号的干扰，检测的漏报率和误报率较高；通过调制摄像头的功率，该方法的检测范围也将受到考验。

基于热量的方法，若摄像机隐藏在其他电器中，则不易被发现，在办公室环境下，办公设备较多，热成像仪具有较大局限性，不能够防止手机等设备的窃拍行为。

基于通信的方法，主要针对长期窃拍的隐藏摄像头，对于屏幕窃拍行为的预防与检测的帮助有限，且在电磁信号复杂的环境下，该方法也具有较大的局限性。

综上，检测摄像头的方法对远距离攻击的抵抗能力都较弱，随着摄像技术的发展，摄像水平越来越高，远距离也可以进行拍摄，经后期处理，内容依旧清晰。

3.3　屏幕水印法

水印技术是有效的数字信息保护手段，在原始信息载体（如文字、图像、视频等）中添加的具有不影响原信息的完整性、可读性，并具有安全性、鲁棒性、隐蔽性的信息称为水印。使用水印进行屏幕防拍摄的方法主要利用水印的特性将含有计算机基本信息或者特殊含义的图像嵌入到屏幕信息中，使之不可分离，水印中可包含计算机基本信息（IP、用户等）或者其他的标示性信息（二维码、图案等）[22]。当屏幕信息被窃拍时，通过提取出的水印可以有效查找出泄漏信息的来源，为追溯提供可靠依据，该方法可以让窃拍者忌惮。

3.3.1　水印的基本原理

水印技术一般包括两个过程，即水印添加和水印提取。原始的水印信息 I_m 一般需进行预处理，使用密钥加密或者转置后，作为水印添加算法的输入，嵌入原始的信息载体中；由水印提取算法提取到的信息经密钥解密后得到水印信息 I_m'，将 I_m 与 I_m' 进行对比，可以发现其来源、真实性或完整性等[22]。具体流程如图 4 所示。

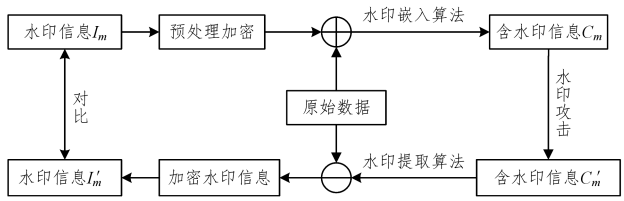

图 4　水印原理流程图

3.3.2　优势

在重要信息的屏幕上嵌入水印进行防窃拍的优势如下：

1）可追溯性，水印信息的嵌入为原始数据被窃拍后的追溯提供了依据，可追溯泄密的计算机、场所、人物等，防范再次发生窃密行为。

2）隐蔽性，水印嵌入后，肉眼一般不可见，需使用算法提取，不会影响原始数据的正常使用。

3）真伪性，当原始数据发生更改后，水印信息也会发生变动，因此依据提取的水印信息可验证原始数据是否被篡改。

4）简易性，水印的嵌入和提取算法较为简单，实现比较容易，并且对原文的使用影响较小[23]。

3.3.3　局限性

该方法仅用于事件发生后进行追溯，无法阻止事件的发生，而且水印技术本身的局限性会给追溯工作造成一定的困难，具体如下。

1）鲁棒性攻击：即直接攻击，直接对水印信息进行去除性

攻击,包括信号处理攻击法和分析攻击法。信号处理攻击方法包括有损压缩,降噪攻击,线性、非线性过滤,扫描打印等;分析攻击方法即删除攻击,删除或者减弱水印信息,包括共谋攻击和多重文档攻击。

2)表达攻击:即同步攻击,指使水印提取算法无法提取到水印信息的攻击,包括旋转缩放、图像裁剪、仿射变化、几何变化等方法。

3)解释攻击:该攻击指攻击者在原水印信息中使用水印嵌入算法加入攻击者水印,在水印提取过程中,可以提取到攻击者的水印信息,进行多种解释,混淆攻击者与所有者[24]。

结束语 随着技术的发展,窃拍手段也在不断改进,窃拍行为越来越不易被察觉。首先是设备小型化,针孔摄像头、微缩相机、纽扣式摄像机不断问世,窃拍设备越来越小。其次是手段多样化,日常中可以用来拍摄的设备越来越多,除了摄像机外,还有各式各样的手机、手表,谷歌眼镜也推出了拍照功能。最后是信号隐蔽化,专业的窃拍设备为防止窃拍行为被发现,加装电子设备电磁信号弱化部件,减少设备的声音与电磁信号。

遏制窃拍行为刻不容缓,而现行的屏幕防窃拍方法有较大的局限性,对于防窃拍的预防能力不足,探索新的防范技术对保护信息系统中的关键信息的安全至关重要。随着智能时代的到来,机器视觉在安防监控、无人车等方面的应用为屏幕防窃拍问题提供了新的思路与方法。

计算机视觉是通过模拟"人"的视觉来分析与处理信息的一门融合了图像处理、模式识别等多方面知识的综合性学科,计算机视觉技术在智能监控、物体识别与分类、运动目标的追踪等方面有较成熟的应用[25-26],计算机视觉的最终目标是机器完全代替人眼去识别事物,并在正确识别的基础上作出决策。设想一种基于计算机视觉技术的防窃拍方法,使用摄像头采集动作视频识别人物的拍照动作与手机,若发现违规行为,则立即保存在读文件并采取措施阻断文件的浏览,同时产生报警并记录违规行为。该方法能够解决传统问题中的大部分局限性。

但基于计算机视觉的方法也有自己的局限性,如对隐蔽性的摄像头无法作出识别,因此未来屏幕防窃拍方法的研究方向是建立一套体系化的防窃拍平台,综合现有的防窃拍方法,形成"预防—防止—追溯"的体系方法。当使用屏幕展示或编辑重要信息时,首先通过摄像头电磁信号检测是否有隐藏并处于工作状态摄像头,应用计算机视觉原理检测并分析是否有窃拍的行为,其次进行整体分析,若发现危险行为,即刻终止屏幕显示行为,并产生预警与日志记录。

随着高科技的发展,拍摄方法呈现出多样性和多变性,为屏幕防拍摄不断带来新的挑战。目前,人工智能技术的发展为屏幕防窃拍方法提供了新的思路与方向,当前防窃拍方法的应用范围较窄,还需要进一步研究。

参 考 文 献

[1] 朱杰.美国 NSA 全球监听和网络窃密行径深度揭秘 看山姆大叔如何玩转"全球监听"[J].中国信息安全,2014(6):80-87.

[2] Risk Based Security. Data Breach Quick-View: An Executice's Guide to 2013 Data Breach Trends[OL]. https://pages.riskbasedsecurity.com/hubfs/Reports/2016_MidYear_DataBreachQuickViewReport.pdf.

[3] 范荣.从黄宇间谍窃密案谈加强保密管理对策[J].保密工作,2016(5):40-42.

[4] 赵飞.智能手机泄密风险分析及安全保密技术方案[J].电子技术与软件工程,2017(2):216.

[5] ROESSLER M. How to find hidden cameras[OL]. http://www.doc88.com/p-9641502582457.html.

[6] TRUONG K N,PATEL S N,SUMMET J W,et al. Preventing camera recording by designing a capture-resistant environment[C]// Proceedings of the 7th International Conference on Ubiquitous Computing. Tokyo,Berlin-Heidelberg:Springer,2005.

[7] GROSGES T. Retro-reflection of glass beads for traffic road stripe paints[J]. Optical Materials,2008,30(10):1549-1554.

[8] YAMADA T,GOHSHI S,ECHIZEN I. Countermeasure of re-shooting prevention against attack with infrared-cut filter[C]// Proc. of IPSJ Symposium on Computer Security(CSS). 2010.

[9] MAHDAVI M,MAHDAVI H,FARSI F. System and method for video recording device detection: US, 20120128330 [EB/OL]. (2012-05-24) [2012-11-15]. http://www.faqs.org/patents/app/20120128330.

[10] FUJIKAWA M,AKIMOTO J,ODA F,et al. Study of Countermeasures for Content Leaks by Video Recording[C]// 2011 Sixth International Conference on Availability, Reliability and Security. 2011.

[11] GURI M, HASSON O, KEDMA G, et al. An Optical Covert-Channel to Leak Data through an Air-Gap[OL]. https://arxiv.org/pdf/1607.03946.pdf.

[12] HUANG H C,FANG W C. Metadata-based image watermarking for copyright protection[J]. Simulation Modeling Practice and Theory,2010,18(4):436-445.

[13] JUNG E H,CHO S Y. A robust digital watermarking system adopting 2d barcode against digital piracy on p2p network[J]. IJCSNS International Journal of Computer Science and Network Security,2006,6(10):263.

[14] PIEC M,RAUBER A. Real-Time Screen Watermarking Using Overlaying Layer[C]// Ninth International Conference on Availability. 2014.

[15] 耿振民,王衍江.一种防止对屏幕拍照的反泄密方法:CN 103390141 A[P]. 2013.

[16] 张文豪,吴怀宇.基于摄像头检测的防盗拍系统开发和算法研究[J].电子设计工程,2013,21(18):48-52.

[17] 汪嘉恒,程雨诗,徐文渊.基于辐射特征的隐藏摄像头检测技术[J].工业控制计算机,2017,30(2):50-52.

[18] 汪嘉恒.面向防拍摄的摄像检测技术[D].杭州:浙江大学,2017.

[19] 褚晶辉,田叶,苏育挺.基于频率约束的相机与屏幕通信隐写算法[J].激光与光电子学进展,2018,55:051003.

[20] 四种屏幕防拍照、截屏、打印等数据泄露水印解决方案[OL]. https://www.leagsoft.com/doc/article/1416.html.

[21] 防范屏幕拍照泄密不再束手无策[OL]. http://www.ip-guard.net/blog/?p=1922.

[22] 吴海涛,詹永照.数字水印技术综述[J].软件导刊,2015,14(8):45-49.

[23] 吴亚坤,邸春红.数字水印技术综述[J].辽宁大学学报(自然科学版),2010,37(3):202-206.

[24] 马颖颖.数字水印攻击方法的一些研究[D].杭州:杭州电子科技大学,2011.

[25] 李彦冬.基于卷积神经网络的计算机视觉关键技术研究[D].成都:电子科技大学,2017.

[26] 杨益平,闵啸.基于计算机视觉的手势识别人机交互技术[J].电子技术与软件工程,2018(12):138-139.