

视频隐私保护技术综述

金 华 朱靖宇 王昌达

江苏大学计算机科学与通信工程学院 江苏 镇江 212000



摘 要 随着视频处理技术的迅速发展及硬件成本的不断降低,监控设备得到了越来越广泛的应用。视频监控普及所带来的隐私问题泄露逐渐成为了研究热点。根据目前视频隐私保护领域的研究现状,将视频隐私保护方法主要分为隐私主体识别、隐私主体保护以及隐私信息管理 3 个阶段,对每个阶段的算法进行分类概述并分析其优缺点,其中视频区域保护作为视频隐私保护领域的重要组成部分,联系视频编码发展历程对保护方法进行了分析和比较。最后探讨了视频隐私保护领域目前存在的问题并对未来的研究方向进行了展望,为视频隐私保护的相关研究提供了参考。

关键词: 视频加密;隐私区域提取;隐私保护;视频编码;数据隐藏

中图法分类号 TP309

Review on Video Privacy Protection

JIN Hua, ZHU Jing-yu and WANG Chang-da

School of Computer Science & Communication Engineering, Jiangsu University, Zhenjiang, Jiangsu 212000, China

Abstract With the rapid development of video processing technology and the continuous reduction of hardware costs, surveillance equipment has become more and more widely used. The leakage of privacy issues brought about by the popularity of video surveillance has gradually become a research hotspot. According to the current research status in this field, video privacy protection methods are mainly divided into three stages: privacy subject identification, privacy subject protection and privacy information management. Each stage algorithm is classified and summarized, and its advantages and disadvantages are analyzed. The privacy region protection is an important part of this field. The protection methods are analyzed and compared in connection with the development of video coding. Finally, the existing problems in the field of video privacy protection are discussed, and the future research direction is prospected, which provides a reference for the related research of video privacy protection.

Keywords Video encryption, Privacy region extraction, Privacy protection, Video coding, Data hiding

1 引言

近年来,随着互联网和多媒体技术的快速发展,以及视频监控的硬件成本、实施成本的不断下降,使视频监控技术得到了广泛应用。视频监控可以使监控者对目标区域实施远程监控,这给日常的治安管理、事故预警、案件侦破等需求带来了极大便利,但越来越多的监控设备也增加了隐私泄露的风险。现实生活中视频泄露的案例并不少见,泄露的隐私信息如果被非法使用,可能会对受害者造成巨大损失和伤害,泄露的信息有些甚至涉及到商业机密和国家安全。因此,视频隐私保护技术具有巨大的应用价值和研究前景。

随着视频监控市场规模的愈发庞大和民众隐私保护观念的成熟,视频监控所带来的负面效应也逐渐受到重视。针对视频的隐私保护策略也引起了国内外学者的热切关注。针对这一跨学科问题,解决途径一般有两方面,除了需要相关法规

的完善,另一方面则要从技术方面入手。Wickramasuriya 等首先提出了监控视频隐私保护系统的概念^[1],在此之后国内外研究者针对这一概念取得了丰硕的成果。总体来说,视频隐私保护可以分为两大步骤,一是隐私主体的识别及隐私区域的提取,如果需要对个体进行选择保护,则需要先进行主体识别,隐私主体识别方法主要包括基于生物特征识别^[2]和基于非生物特征识别^[3-4],对隐私区域的提取的主要方法有人脸检测^[5-6]、运动物体检测^[7]等,有些方法还在此基础上结合了目标跟踪^[8]方法来提取隐私区域;二是对隐私区域进行保护,根据其和视频编码的关系可以分为编码前保护、结合编码保护和编码后保护。近年来,随着编码标准的不断发展,结合视频编码对隐私区域进行保护成为了视频隐私区域保护的研究热点。与视频加密研究的不同点在于,其对视频隐私区域保护的同时还要满足正常的视频监控任务,即保证视频其他区域的视觉完整性。因此,对于结合编码的隐私区域保护

到稿日期:2020-12-03 返修日期:2021-04-09 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:国家自然科学基金(61902156);国家重点研发计划(2017YFC1600804);江苏省自然科学基金(BK20180860)

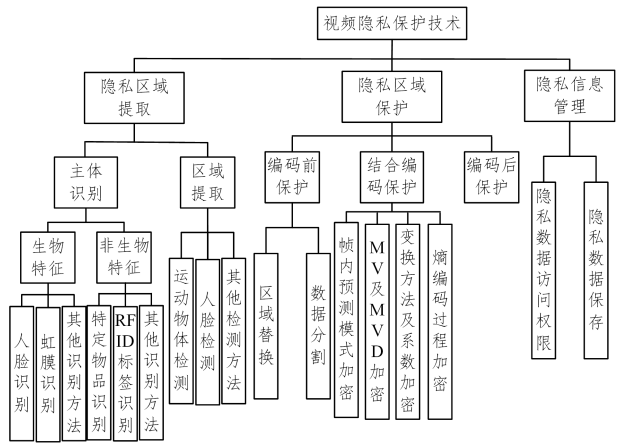
This work was supported by the National Natural Science Foundation of China(61902156), National Key Research and Development Program of China(2017YFC1600804) and Natural Science Foundation of Jiangsu Province(BK20180860).

通信作者:金华(jinghua@ujs.edu.cn)

方法,还需要考虑误差漂移等问题^[9]。因为视频隐私保护效果需要从多角度分析评价,缺乏统一的评价效果,所以有些学者还研究了隐私保护评价体系的建立。

2 视频隐私保护技术

视频隐私保护一般需要满足以下基本特性,保护视频信息的安全性,即破译密码所付出的代价远大于破译者能承受的代价时,通常认为是安全的,并且执行隐私保护后的视频和原视频相比,需要考虑加密时间、存储空间的变化,以及视频的格式兼容性。如图 1 所示,视频隐私保护方案要从以下 3 个方面进行区分:视频隐私主体的识别及隐私区域的提取、隐私区域保护和隐私信息管理。



2.1 隐私主体的识别及隐私区域的提取

隐私保护的第一步是对隐私区域进行识别和提取,有些隐私保护方案不对主体进行识别,而是直接在视频中检测相应的隐私区域(如面部、身体轮廓等)并对其进行提取,但考虑到实用性,部分方案选择先对隐私主体进行识别,判断其是否需要保护,再决定隐私区域的提取。

2.1.1 隐私主体的识别

通常情况下,隐私主体为人类或能反映个人身份信息的物体(如车牌、携带的配饰等),根据不同的应用场景,隐私主体识别方法一般分为基于生物特征的识别以及基于非生物特征的识别。

(1) 基于生物特征的识别

视频中的隐私信息的隐私主体一般为人类,因此,基于生物特征识别隐私主体并结合主体跟踪技术在视频中确定保护对象具有较高的实用性,随着生物特征识别技术的不断进步,基于面部、虹膜等特征的隐私保护主体识别取得了许多成果^[10],识别的安全性、识别效率也都在不断提高。与其他基于非生物特征的识别相比,生物特征信息具有不可复制性,并且对于识别主体而言可以实现被动识别,对主体行为的影响较小,实用性较高。

对具体的生物特征而言,目前主体识别中最为成熟的是基于面部的识别,一方面,面部信息相对于其他生物特征(如虹膜、指纹等)属于弱隐私生物特征,另一方面,监控视频具有

低分辨率、光照条件不受控制等特征,但面部识别也能保证一定的准确性,这使得面部识别在现实场景中有较高的实用性。与传统的面部识别方法相比,其虹膜识别的精确度更高,传统的虹膜取样的方法需要近距离采集虹膜信息,但目前已经可以较远距离识别虹膜信息^[11],其他识别方法(如语音、红外等)一般应用于特定场景^[12-13],该方法既需要个体对采集信息设备作出相应反馈,又需要在摄像头侧增加额外的硬件设备,这限制了此类识别方法在隐私保护方面的应用。

(2) 基于非生物特征的识别

相比基于生物特征进行识别,根据非生物特征进行识别更具有通用性,可以预先设定一种或多种特征标记进行识别。文献[4]将工人佩戴的特定颜色的安全帽作为主体判断标记或将特定服装作为识别标记。文献[3]将特定色彩的标签作为隐私保护判断的标记,并由多个摄像机配合以减小遮挡的影响。文献[14]中人员配备 RFID 标签作为特征识别的标记。这些方法虽然识别效率较高,并且还提供了追踪的功能,但此类特征标记不具有唯一性,且与隐私主体之间的关联性较弱,因此在实际应用中具有较大的局限性。

2.1.2 隐私区域的提取

对于视频中的隐私区域,可以识别出需要隐私保护的主体之后再对其进行保护,也可以直接进行感兴趣区域检测并对其进行保护,目前在视频隐私保护研究中主要的隐私区域检测方法有运动物体检测和人脸检测。

(1) 运动物体检测

监控视频中的隐私主体大多为运动物体,因此,有较多的隐私保护方案直接将运动物体作为隐私保护的對象^[15]。监控视频中准确地检测运动目标是后续对隐私主体进行提取和保护的基础。直接基于运动的方法^[16]虽然可以很好地提取运动主体,但一方面长时间静止的人类、车辆等情况容易造成误判,另一方面实时运动分离对监控视频的大量数据而言,计算量较大。考虑到大多数监控设备是静态存在的,监控视频背景具有较高的冗余度,因此有些场景适合将监控视频分为背景和前景,目前有较多的方案能够快速准确地建立背景模型,从而准确提取出目标前景并进行保护^[17]。

(2) 人脸检测

面部区域信息作为反映个人身份的重要依据,快速准确地检测视频中的人脸区域对隐私区域的提取至关重要,相关的研究成果也较为丰富^[18-19]。

有些场景仅对面部进行保护,无法隐藏目标信息,根据其他信息也可以辨认出人员的身份信息(如发型、衣着、配饰等)^[20]。为提高隐私保护效果,有部分方案选择对人体皮肤区域^[21]或整个身体轮廓^[12]进行保护。

在视频隐私保护技术中,对于隐私主体的鉴别和隐私区域的提取方法有很多,但大多数方法提取的区域都是面部、身体轮廓或运动物体,具体提取方法则需要根据使用场景、安全性要求来选择。

2.2 隐私区域保护方法

由于监控视频的数据量大、数据结构特殊,需要对视频数据压缩后进行存储或传输,因此,对隐私区域进行保护时需要考虑视频编码对隐私区域保护方法的影响,尤其是目前使用

较为广泛的 H. 264 和 HEVC 编码。按照隐私区域保护与编码的关系,视频隐私区域保护可分为编码前保护、结合编码保护和编码后保护。

2. 2. 1 编码前保护

编码前保护指在视频数据被压缩前对隐私区域进行保护,这种方法的基本原理比较简单,将未进行编码的视频中的隐私区域进行保护后再进行视频编码传输或存储,该方法独立于视频编码,可以与不同编码方式的隐私保护系统兼容,此类方法的研究主要分为以下两个方面。

(1)隐私区域替换

早期有很多方法直接在像素域对隐私区域实现替换,从而实现隐私区域的不可见,具体方法有隐私区域指数时空域模糊^[22]、高斯模糊^[23]、面部替换^[24]、图像扭曲^[5]、伪随机置换^[25]等,由于后续视频压缩编码依赖视频帧的像素相关性,而密文图像的像素相关性一般较低,因此降低了压缩效率,并且该类方案在视频编码后一般会面临视频隐私区域存在明显的视觉质量受损以及处理过程不可逆的问题。图 2 给出了部分编码前隐私保护方法的表现效果。

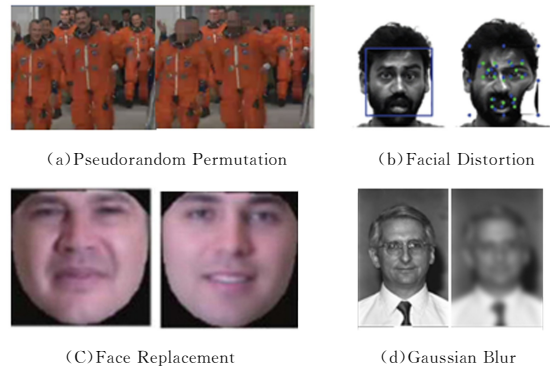


图 2 隐私区域的替换效果

Fig. 2 Privacy region image replacement

(2)基于数据分割的保护

此类方法将视频信息分成多个部分,且每个部分都进行独立处理,将所有部分数据结合才可以恢复原始画面。目前已有针对监控视频分布式处理的隐私保护方法,以实现视频信息的安全处理^[26]。但这种方法需要较多的处理器及相应的存储空间,并且若分割的某个部分出现问题,则整个视频信息将难以恢复。

2. 2. 2 结合编码保护

考虑到独立于视频编码加密方法的缺点,现有加密算法大多与视频编码相结合,即对视频信息重建过程中具有重大意义的数据进行加密。一般使用已有或改进的加密算法在视频编码过程中选择合适的数据进行加密,从而达到视频加密的目的。视频隐私区域的整体数据量虽然较大,但编码过程中需要加密的敏感数据较少,减少了加密过程中对硬件的需求,并且加密后的视频文件具有格式兼容性,能够兼顾加密的安全性和加密效率,较好地满足实时性的要求。图 3 为视频编码过程中可选择加密位置示意图,主要分为帧内预测模式加密、运动矢量及运动补偿加密、变换方式及变化系数加密和熵编码过程加密。

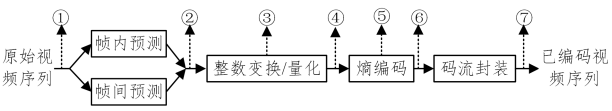


图 3 编码过程加密位置示意图

Fig. 3 Schematic diagram of encryption position during encoding

(1)帧内预测模式加密

在视频编码中,帧内预测模式表示关键帧像素间的预测信息,是关键帧解码重建的重要依据。文献[27]首次提出对帧内预测模式加密,对帧内预测模式加密后将会引起错误扩散,后续的 P、B 帧以此帧作参考播放视频时,将出现画面失真,从而达到保护隐私的目的,并且加密算法不会改变视频压缩率。但算法使用的是固定长度的伪随机序列作为密钥,并且帧内预测模式的数量有限,因此其安全性较低。文献[28]使用混沌伪随机序列作为密钥对帧内预测模式进行加密,相比文献[27],其提高了一定的安全性,但仍存在加扰空间不足的缺点。文献[29]为扩大加扰空间,采用密钥控制的循环序列对帧内预测模式进行二次加密,该方法提高了安全性,但视频码率会有轻微变化,并且视频中的 P、B 帧也缺乏相应的保护。在实际方案中,通常结合视频其他部位的加密来提高安全性。

(2)运动矢量加密

运动矢量是视频解码的重要数据,用于表示视频帧中图像块的位移信息。Zheng 等^[30]提出了一种在无图形信息的前提下仅使用运动矢量就可以恢复包含对象轮廓信息的低分辨率视频的方法,表明了运动矢量对视频解码重建的重要性。在对运动矢量加密的方案中,较多的是对运动矢量符号位进行加密,文献[31]首先提出对运动矢量差符号位加密,但如果将运动矢量符号位加密作为主要加扰手段将无法防止运动矢量恢复(MVR)攻击^[30],不适用于对安全需求较高的场景。因此,运动矢量差符号位加密一般不会单独用于视频加密,而是结合其他部位加密用于保证安全性^[32-35]。除了对符号位进行加密外,还可以对运动矢量的数值和方向进行加密,但直接加密运动矢量的值可能会导致比特率的增加。

(3)变换方式及变化系数加密

视频的变换编码指将视频空间中像素表示的信息经变化后在变换域中进行表达,视频进行变换编码后,可以改变数据的分布形式,减少数据量。针对变换过程的加密主要有变换方式加密和变换系数加密。变换方式加密指更换编码器指定变换方式的加密方法,文献[36]提出用 unit 变换取代 H. 264 指定的 DCT 变换,从而实现视频加密。因为变换过程本身也是压缩编码的一部分,且选用的变换方式的编码效率与原变换方式相似或者轻微下降,所以使用此类方法则不再需要额外的加密过程,降低了计算复杂度,但加密后视频视觉安全性有限。文献[37]使用改进的变换方式提高了加密的视频视觉安全性,但对于硬件解码器芯片,需要对编解码器的变换模块做相应修改,实现成本较高^[38]。除了更改变换方式,还可以对变换系数加密,主要方法有对变换系数位置置乱^[39],但由于后续需要进行变换系数扫描,位置置乱后的数据会改变数据原有的分布规律,影响编码性能。还可以对

变换系数符号位加密^[30],对符号位加密的计算代价小,对后续编码率的影响也较小,但易受明文攻击,安全性有限,因此常作为增加加密安全性的补充手段。此外,还有方法对变换系数的幅值进行直接加密^[40]。

(4) 熵编码过程加密

在视频压缩标准中,熵编码过程在视频信号的压缩和码流的组织过程中有着重要作用,是视频压缩编码的最后阶段。熵编码模块主要利用待编码符号的概率分布高效地去除信源符号间的冗余信息。在结合视频编码隐私保护方法中,在熵编码前加密的方法一般会对视频压缩率有影响,在熵编码完成后对视频加扰,一般要处理的数据量较大,因此,有较多的方法研究在熵编码过程中对隐私信息进行保护。熵编码过程中的加密方法主要是对编码过程中的数据进行加密,此外,还有方法将熵编码过程中的霍夫曼码表修改后进行使用,以实现视频加密^[41-42]。

(5) 误差漂移

误差漂移指在结合视频编码的隐私区域保护方法中,加密后区域的数据可能用于其他宏块参考的情况。如图4所示,如果解码端不对受保护区域解密,那么重构的视频加密区域外会出现视频质量下降的问题。误差漂移是结合编码对视频部分区域进行加密的过程中需要解决的关键问题。



图4 误差漂移现象

Fig. 4 Error drift

为避免误差漂移对非隐私区域的影响,文献[43]将视频帧中未加扰宏块与已加扰宏块独立编码,即不进行互相参考,以避免误差漂移。文献[44]通过 H. 264 的灵活排序机制(FMO)将视频帧加扰宏块和非加扰宏块分入不同切片组,由于编码时不会跨切片组预测,因此实现了对帧内误差漂移的抑制。文献[45]利用 HEVC 中 Tile 单元独立编码的特性,对包含感兴趣区域的 Tile 进行加密,以实现帧内误差漂移的抑制。也有方法通过预测受限的方法来实现对误差漂移的抑制,对于 H. 264 编码方式,文献[46]的主要思想是在运动估计期间限制搜索区域,使搜索对象不包括加扰区域,主要提出了两种实现方法,即模式受限帧内预测和搜索窗口受限运动估计。文献[47]在此基础上通过边界强度限制解决滤波器的方法,进一步消除了误差漂移。

在视频编码过程中,加密数据的数据量虽然较小,但其对视频重建播放非常重要,因此需要对帧内预测模式、运动矢量和运动补偿以及残差数据、熵编码过程中的数据进行了加密,对这几类数据进行合理的加密能够保持高计算效率和格式兼容,但对单一数据加密的安全性较低。因此,目前很多视频加密方案都是使用多种关键数据共同加密来提高安全性。此外,还有一些其他方法,例如,使用随机的置乱序列来代替编码器指定的扫描顺序(如 zigzag 扫描)对变换系数进行扫

描^[48],这种方法的加扰速度快,不影响实时传输,但经过加密的视频压缩后,码流显著增加,缺乏实用性。可以看出,各种现有的压缩域加密方案都是在安全性和加密效率以及编码效率之间的折衷,在实际应用中可以根据不同的安全性要求,选择加密不同数量的敏感数据,从而满足相应安全等级的要求。

就保护方法发展历程而言,视频加密方法和视频压缩标准的发布密切相关,早期多在像素域对视频区域进行加密,但从 1993 年引入 MPEG-1 视频编码以来,很多结合视频编码的信息保护方法相继出现^[49],在 H. 264 之前,存在许多针对 MPEG-2 或 MPEG-3 视频编码的视频加密方法,大多数方法是对变换系数和运动矢量进行加密。2003 年初 H. 264 标准发布后,引入的一些新的编码方法和结构,例如,帧内预测模式、FMO 等都可以结合到视频感兴趣区域的加密算法中^[27,50],在相同的视频质量下 2013 年之后发布的 HEVC 视频标准比 H. 264 拥有更低的码率,并且支持并行处理,同时也涌现出了一些针对此标准的加密算法^[51-53]。因此,应充分研究和利用视频压缩编码的特点,在满足安全性的前提下,尽可能地减少加密数据。

2.2.3 编码后保护

对于编码后的视频,也可以进行隐私保护,即对压缩后的视频重定位隐私区域并进行保护,相对于结合编码保护的方法,此类方法的加密过程不需要对标准编码器做修改。文献[54]提出了一种轻量级视频隐私保护方法,对视频关键帧的隐私区域进行提取并加密,之后对去除隐私区域的新视频帧进行重新编码。但此方法需要对关键帧感兴趣区域去除后的视频进行二次编码,实时性表现一般。

2.2.4 基于数据隐藏的方法

基于数据隐藏的方法指对隐私信息进行擦除,将擦除的隐私信息作为水印嵌入到载体视频中,并对原隐私区域使用视频背景恢复或视频修复技术来补全场景。如图5所示,左图为未擦除的视频图像,右图为隐私信息擦除并补全视频的图像,如果是授权解码端解码则可以恢复包含隐私信息的视频。



图5 图像恢复

Fig. 5 Image restoration

文献[55]提出了一种基于视觉模型的压缩域视频隐藏方法,用于保护监控视频中的隐私信息,并用背景模型填补视频帧中提取隐私区域后的无信息部分。但该方法将所有隐私信息压缩后全部嵌入到视频中,需要嵌入的数据量较大,实时性表现一般。文献[56]将人脸区域作为需要保护的對象嵌入到视频中,并用虚拟人脸覆盖在原始人脸区域,为解决信息隐藏较大的荷载问题,使用了基于主动外观模型(AAM)进行隐私信息的提取和恢复,但该方法需要一系列的面部图片来训练统计主动外观模型(AAM)。文献[57]将 DWT 变换系数嵌入视频中,可以显著减少需要嵌入视频的数据量。

相比其他方法,结合视频修复的数据隐藏方法不仅能够隐藏隐私数据在视频中的位置,通过视频修复还能隐藏隐私对象在视频场景中的信息,具有较高的实际应用意义。但目前对于大容量的视频数据隐藏需要权衡嵌入后视频的视觉品质以及带宽增加的问题。对于视频修复技术,如果需要保证良好的恢复效果,则需要对监控视频所在的场景有一定限制,如果出现背景变化较大、需要修补的隐私区域过大、人物运动轨迹没有规律性等问题,当前的视频修复技术很难保证良好的视觉效果。

2.3 隐私数据安全

目前大多数隐私保护方案较多关注对视频隐私区域的保护,但隐私数据的管理对于保证隐私信息的安全性也同样重要。一方面需要考虑隐私数据进行访问时的验证问题,即隐私数据访问权限问题,另一方面则是隐私数据保存问题。

目前大多数方法都是采用简单的访问控制模型,其安全性有限。文献[17]利用开发的隐私数据管理系统将隐私数据的访问权限安全地授予经过了身份验证的客户端。文献[2]提出了以用户为中心的隐私信息管理系统,该系统基于混淆电路虹膜验证方式匿名验证用户身份,并实现了细粒度的访

问控制,满足了对个体隐私信息进行独立管理的需求。除了访问权限控制外,隐私数据的安全存储也很重要,文献[12,58]将隐私数据分成多个部分并发送给不同的服务器进行处理,以实现数据的安全存储。

2.4 典型方案分析及比较

本节从整体角度对视频隐私保护技术进行分析,如表1所列,对于隐私保护方案的隐私区域提取方法,因为面部信息在监控视频中是确认身份信息的主要特征,并且视频中的面部检测技术目前也很成熟,所以很多方案选择面部信息作为隐私区域,而有些方案对安全性要求较高,选择对整个身体轮廓进行保护。部分场景并不需要保护视频中的全部人员,因此需要对视频中的人员进行身份识别,可以根据相应的身份特征确定是否需要保护。确定保护区域后,需要对相应区域进行保护,根据保护方法与编码的关系又可以分为3类。编码前保护方法,比较常见的是在像素域对视频区域进行加密,实现原理简单,并且可以借鉴丰富的图像加密成果,该方案由于独立于编码器来实现保护,可以方便兼容不同编码的监控系统。但此类方案保护的视频一般不可逆,并且对于隐私区域较大的情况,该方法需要加密的计算量较大,加密效率较低。

表 1 典型方案
Table 1 Typical method

文献	年份	隐私区域提取	隐私区域保护	应用场景	编码
文献[5]	2013 年	人脸检测	编码前保护,人脸图像扭曲	视频监控系统	未涉及
文献[2]	2017 年	虹膜识别结合运动物体检测	编码前保护,隐私区域替换	视频监控系统	未涉及
文献[55]	2005 年	RFID 识别结合运动物体检测	数据隐藏,基于背景的视频修复	医院或公司等密闭环境	H. 263
文献[59]	2016 年	假设区域已知	编码后保护,变换系数和帧内预测模式比特流加密	视频无损的隐私保护系统	H. 264
文献[56]	2007 年	人脸检测	数据隐藏,人脸替换	实时视频监控系统	MPEG-2
文献[50]	2013 年	人脸检测	结合编码保护,熵编码过程加密部分编码数据	视频监控系统	H. 264
文献[45]	2015 年	假设区域已知	结合编码保护,熵编码过程加密部分编码数据	视频监控系统	HEVC
文献[54]	2018 年	假设区域已知	编码后保护,提取 I 帧隐私区域加密	低运算成本的视频监控系统	H. 264
文献[12]	2019 年	身体轮廓	编码前保护以及数据分布式存储处理	视频监控系统	H. 264
文献[52]	2018 年	假设区域已知	结合编码保护,熵编码过程加密部分编码数据	多媒体信息安全	HEVC

目前使用得较多的是结合视频编码实现隐私区域的保护,通过在编码阶段选择对视频重建过程中比较重要的数据进行加密,使视频隐私区域不能清晰解码,从而实现隐私区域的保护。此类方案的加密数据量相对较小,并且加密后视频格式的兼容性高,因此有较多方案选择此类保护方法。并且随着新编码标准的发布和使用,寻找新标准内适合加密的数据也成为了研究人员关注的热点。还有方案对已编码视频解码后确定隐私区域进行保护,但加密处理后一般还需要再次编码,会影响监控系统的实时性,因此此类方案较少使用。

3 视频隐私保护技术的难点与趋势

视频隐私保护是融合了多学科知识、具有良好发展前景的学科。尽管近年来视频隐私保护领域快速发展,取得了很多研究成果,很多性能优异的隐私保护方法不断出现,但目前

仍存在许多难点问题需要解决,具体包括以下几个方面。

(1)视频隐私保护算法效果评估问题。目前对隐私保护技术的保护效果采用的评价指标存在局限性,缺乏统一的评价标准。有的文献从密码安全性角度进行分析,即隐私保护算法的抗攻击能力,还有的从视觉安全性角度进行分析,即从主观评价指标和客观评价指标这两方面进行分析。主观评价指标的基础是人体视觉系(HVS),虽然主观评价是视觉安全性评价的重要指标,但需要较长的实验时间及较多的实验人数,评价结果会受到较多因素的影响(如个体差异、评价的图像类型等),并且结果不具备可复现性。此外,效果评估还要考虑算法的计算复杂度、隐私保护后码流格式的兼容性以及对压缩率的影响等。客观全面评价指标的建立有助于推动视频隐私保护技术的发展,近年来也涌现出了一些关于这方面的研究^[60-63]。

(2)为保证监控系统的实时性,需要考虑视频隐私保护安全性和计算复杂度之间的平衡问题。影响加密算法计算复杂度的因素主要涉及两个方面,一是选择的需要加密的数据,目前一般选择在编码过程中的关键数据或已编码的视频数据进行加密;二是选择的加密算法本身的计算复杂度,加密算法大多是已有算法或其他改进算法。通常来说,在加密数据确定的情况下,算法的计算复杂度和安全性是成正比的,但还需根据实际的应用场景来平衡安全性和计算复杂度。此外,如果对擦除隐私部位的视频区域进行修复,则会更大程度地影响监控系统的实时性。

(3)视频隐私保护算法的硬件实现问题。现有的视频隐私保护实验方法大多基于计算机设备进行视频隐私保护算法的实现。但在有些场景下,隐私保护方法需要集成到监控设备端,监控设备摄像头的内存资源和计算能力有限,隐私保护所涉及的目标检测、识别等算法和加密算法需要协同执行,导致一些隐私保护方法无法满足实际应用。因此,对硬件设备友好的隐私保护方法才能更好地满足实际需求。

(4)隐私保护和行为分析的矛盾问题。隐私信息的定义并不明确,对不同的人、不同的场景以及不同的文化背景都有着不同的定义。大多情况下与个人身份信息相关的画面定义为隐私信息,扩大视频中的保护区域可以更好地保护人员的隐私,但隐私保护不仅需要保护被监视者的隐私信息,还需要满足工作人员或智能识别系统对视频内人员进行行为分析以及异常事件检测的任务,在公共安全需求和个人隐私保护之间达到平衡。因此,隐私保护方案需要针对实际情况细化应用场景,才能更好地满足多元化的应用需求。

结束语 随着民众隐私意识的逐渐成熟和相关法规的不断完善,视频隐私保护方法展现了巨大的应用潜力,受到了越来越多研究人员的关注。本文在前人研究的基础上,对视频隐私保护的研究成果进行了全面概述。将隐私保护算法大致分为两个步骤,一是隐私主体识别与追踪,分为基于运动物体识别、基于生物特征识别和非生物特征识别,并分析了相关方法的优缺点;二是对隐私主体进行保护,按保护方法与编码的关系分为3类,并对每类方法的典型算法进行了分析。该领域的相关算法虽然较多,但其中大部分方法未考虑到现实场景的硬件环境以及复杂的应用场景,在现实环境中的应用很多方法都具有较大的局限性。最后分析了目前本领域的难点并预测了未来的研究方向。

参 考 文 献

- [1] WICKRAMASURIYA J, DATT M, MEHROTRA S, et al. Privacy protecting data collection in media spaces[C]// Proceedings of the 12th ACM International Conference on Multimedia. 2004: 48-55.
- [2] LUO Y, CHEUNG S C S, LAZZERETTI R, et al. Anonymous subject identification and privacy information management in video surveillance[J]. International Journal of Information Security, 2017, 17(3): 261-278.
- [3] ZHAO Z, CHEUNG S C. Multi-camera surveillance with visual tagging and generic camera placement[C]// IEEE International Conference on Distributed Smart Cameras. 2007: 259-266.
- [4] SCHIFF J, MEINGAST M, MULLIGAN D K, et al. Respectful cameras: detecting visual markers in real-time to address privacy concerns[C]// IEEE/RSJ International Conference on Intelligent Robots & Systems. 2009: 65-89.
- [5] KORSHUNOV P, EBRAHIMI T. Using warping for privacy protection in video surveillance[C]// 18th International Conference on Digital Signal Processing (DSP). 2013: 1-6.
- [6] MARTÍNEZ-PONTE I, DESURMONT X, MEESSEN J, et al. Robust human face hiding ensuring privacy[C]// 6th International Workshop on Image Analysis for Multimedia Interactive Services. 2005: 4.
- [7] ZHAO W, QIN S. A new method for target detection based on analysis of motion vector field in dynamic video scene[J]. Proceedings of SPIE the International Society for Optical Engineering, 2009, 7495: 4264-4267.
- [8] ZHANG P, KALLIVAYALIL T, EMMANUEL T, et al. Privacy preserving video surveillance using pedestrian tracking mechanism[C]// Proceedings of the 2nd ACM Workshop on Multimedia in Forensics, Security and Intelligence ACM. 2010: 31-36.
- [9] WANG Y, O'NEILL M, KURUGOLLU F. Privacy region protection for H. 264/AVC by encrypting the intra prediction modes without drift error in I frames[C]// IEEE International Conference on Acoustics. 2013: 2964-2968.
- [10] LUO Y, CHEUNG S C. Privacy information management for video surveillance [C]// Conference on Biometric and Surveillance Technology for Human and Activity Identification X. 2013: 871207. 1-871207. 7.
- [11] LEE Y, MICHEALS R J, FILLIBEN J J, et al. VASIR: An open-source research platform for advanced iris recognition technologies[J]. Journal of Research of the National Institute of Standards & Technology, 2013, 118: 218-259.
- [12] MEGHERBI N, AMBELLOUIS S, COLÔT O, et al. Joint audio-video people tracking using belief theory[C]// IEEE Conference on Advanced Video & Signal Based Surveillance. 2005: 135-140.
- [13] KUMAR P, MITTAL A, KUMAR P. A multimodal audio visible and infrared surveillance system (MAVISS) [C]// International Conference on Intelligent Sensing & Information Processing. 2005: 151-156.
- [14] CHEUNG S C S, VENKATESH M V, PARUCHURI J K, et al. Protecting and Managing Privacy Information in Video Surveillance Systems[M]// Protecting Privacy in Video Surveillance. London: Springer, 2009: 11-33.
- [15] MARTIN K, PLATANOTIS K N. Privacy protected surveillance using secure visual object coding[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2008, 18(8): 1152-1162.
- [16] ZHOU X, YANG C, YU W. Moving object detection by detecting contiguous outliers in the low-rank representation[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2011, 35(3): 597-610.
- [17] DU L, ZHANG W, FU H, et al. An efficient privacy protection scheme for data security in video surveillance[J]. Journal of Visual Communication & Image Representation, 2019, 59(2): 347-362.

- [18] BAN Y, KIM S K, KIM S, et al. Face detection based on skin color likelihood[J]. *Pattern Recognition*, 2014, 47(4): 1573-1585.
- [19] DEY A. A contour based procedure for face detection and tracking from video[C]// *Proceedings of International Conference of Recent Advances in Information Technology*. 2016: 483-488.
- [20] ERDÉLYI Á, WINKLER T, RINNER B. Privacy protection vs. utility in visual data-An objective evaluation framework[J]. *Multimedia Tools and Applications*, 2018, 77(2): 2285-2312.
- [21] JAIRATH S, BHARADWAJ S, VATSA M, et al. Adaptive skin color model to improve video face detection[J]. *Advances in Intelligent Systems & Computing*, 2016, 390: 131-142.
- [22] AGRAWAL P, NARAYANAN P J. Person de-identification in videos[C]// *Asian Conference on Computer Vision*. 2009: 266-267.
- [23] DUFAUX F, EBRAHIMI T. A framework for the validation of privacy protection solutions in video surveillance[C]// *Proceedings of IEEE Conference on Multimedia and Expo*. 2010: 66-71.
- [24] NEWTON E M, SWEENEY L, MALIN B. Preserving privacy by de-identifying face images[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2005, 17(2): 232-243.
- [25] CARRILLO P, KALVA H, MAGLIVERAS S. Compression independent reversible encryption for privacy in video surveillance[J]. *EURASIP journal on information security*, 2009, 2009(2): 1-13.
- [26] UPMANYU M, NAMBOODIRI A M, SRINATHAN K, et al. Efficient privacy preserving video surveillance[C]// *2009 IEEE 12th International Conference on Computer Vision*. 2009: 1639-1646.
- [27] AHN J, SHIM H J, JEON B, et al. Digital video scrambling method using intra prediction mode[M]// *Advances in Multimedia Information Processing (PCM 2004)*. 2004: 386-393.
- [28] JIANG J G, LI Y, LIANG L W. Research and improvement of the video encryption algorithm for H. 264[J]. *Acta Electronica Sinica*, 2007, 35(9): 1724-1727.
- [29] JIANG J, XING S, QI M. An intra prediction mode-based video encryption algorithm in H. 264[C]// *International Conference on Multimedia Information Networking & Security*. 2009: 478-482.
- [30] ZHENG L, XUE L. Motion vector encryption in multimedia streaming[C]// *International Multimedia Modelling Conference*. 2004: 64-71.
- [31] SHI C, BHARGAVA B. Efficient MPEG video encryption algorithm[C]// *IEEE Symposium on Reliable Distributed Systems*. 1998: 381-386.
- [32] LIAN S, LIU Z, REN Z, et al. Secure advanced video coding based on selective encryption algorithms[J]. *IEEE Transactions on Consumer Electronics*, 2006, 52(2): 621-629.
- [33] IKENAGA T, GOTO S. A partial scramble scheme for H. 264 video[C]// *7th International Conference on Asic*. 2013: 802-805.
- [34] SU P C, HSU C W, WU C Y. A practical design of content protection for H. 264/AVC compressed videos by selective encryption and fingerprinting[J]. *Multimedia Tools & Applications*, 2011, 52(2/3): 529-549.
- [35] PENG F, GONG X Q, LONG M, et al. A selective encryption scheme for protecting H. 264/AVC video in multimedia social network[J]. *Multimedia Tools & Applications*, 2016, 76(3): 3235-3253.
- [36] YEUNG S, ZHU S, ZENG B. Partial video encryption based on alternative integer transforms[C]// *Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS)*. 2010: 933-936.
- [37] YEUNG S K A, ZHU S, ZENG B. Design of new unitary transforms for perceptual video encryption[J]. *IEEE Transactions on Circuits & Systems for Video Technology*, 2011, 21(9): 1341-1345.
- [38] SHAHID Z, PUECH W. Visual protection of HEVC video by selective encryption of CABAC binstrings[J]. *IEEE Transactions on Multimedia*, 2014, 16(1): 24-36.
- [39] ZENG W, LEI S. Efficient frequency domain selective scrambling of digital video[J]. *IEEE Transactions on Multimedia*, 2003, 5(1): 118-129.
- [40] LEE H J, NAM J. Low complexity controllable scrambler/de-scrambler for H. 264/AVC in compressed domain[C]// *Acm International Conference on Multimedia*. 2006: 93-96.
- [41] ZHOU J T, LIANG Z Q, CHEN Y, et al. Security Analysis of Multimedia Encryption Schemes Based on Multiple Huffman Table[J]. *IEEE Signal Processing Letters*, 2007, 14(3): 201-204.
- [42] XIE D, KUO C. Enhanced multiple Huffman table (MHT) encryption scheme using key hopping[C]// *2004 IEEE International Symposium on Circuits and Systems*. 2004: 568-571.
- [43] DUFAUX F, EBRAHIMI T. Scrambling for privacy protection in video surveillance systems[J]. *IEEE Transactions on Circuits & Systems for Video Technology*, 2008, 18(8): 1168-1174.
- [44] DUFAUX F, EBRAHIMI T. H. 264/AVC video scrambling for privacy protection[C]// *2008 15th IEEE International Conference on Image Processing*. 2008: 1688-1691.
- [45] FARAJALLAH M, HAMIDOUCE W, DEFORGES O, et al. ROI encryption for the HEVC coded video contents[C]// *2015 IEEE International Conference on Image Processing (ICIP)*. 2015: 3096-3100.
- [46] TONG L, DAI F, ZHANG Y, et al. Restricted H. 264/AVC video coding for privacy region scrambling[C]// *2010 IEEE International Conference on Image Processing*. 2010: 2089-2092.
- [47] DAI F, TONG L, ZHANG Y, et al. Restricted H. 264/AVC video coding for privacy protected video scrambling[J]. *Journal of Visual Communication & Image Representation*, 2011, 22(6): 479-490.
- [48] TANG L. Methods for encrypting and decrypting MPEG video data efficiently[C]// *Proceedings of the fourth ACM international conference on Multimedia*. 1997: 219-229.
- [49] BHARGAVA B, SHI C, WANG S. MPEG video encryption algorithms[J]. *Acm Multimedia*, 1998, 24(1): 57-79.
- [50] PENG F, ZHU X W, LONG M. An ROI privacy protection

- scheme for H. 264 video based on FMO and Chaos[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(10): 1688-1699.
- [51] TEW Y, MINEMURA K, WONG K S. HEVC selective encryption using transform skip signal and sign bin[C]// Asia-Pacific Signal & Information Processing Association Summit & Conference. 2015:963-970.
- [52] TAHA M A, SIDATY N, HAMIDOUCHE W, et al. End-to-End Real-Time ROI-Based Encryption in HEVC Videos[C]// 2018 26th European Signal Processing Conference (EUSIPCO). 2018:171-175.
- [53] HAMIDOUCHE W, FARAJALLAH M, SIDATY N, et al. Real-time selective video encryption based on the chaos system in scalable HEVC extension[J]. Signal Processing Image Communication, 2017, 58:73-86.
- [54] ZHANG X, SEO S H, WANG C. A lightweight encryption method for privacy protection in surveillance videos[J]. IEEE Access, 2018, 6:18074-18087.
- [55] ZHANG W. Hiding Privacy information in video surveillance system[C]// Processing of IEEE International Conference on Image Processing. 2005:868-871.
- [56] YU X, BABAGUCHI N. Privacy preserving : hiding a face in a face [M] // Computer Vision-ACCV 2007. Berlin: Springer, 2007:651-661.
- [57] LI G, ITO Y, YU X, et al. Recoverable privacy protection for video content distribution[J]. EURASIP Journal on Information Security, 2009, 200(3):293031.
- [58] DU L, LI Y. Privacy preserving for human object in video surveillance via visual cryptography[C]// Proceedings 2014 IEEE International Conference on Security, Pattern Analysis, and Cybernetics (SPAC). 2014:80-85.
- [59] MA X, ZENG W K, YANG W T, et al. Lossless ROI privacy protection of H. 264/AVC compressed surveillance videos[J]. IEEE Transactions on Emerging Topics in Computing, 2016, 4(3):349-362.
- [60] NAWAZ T, FERRYMAN J. An annotation-free method for evaluating privacy protection techniques in videos[C]// 2015 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). 2015:1-6.
- [61] KORSHUNOV P, MELLE A, DUGELAY J L, et al. Framework for objective evaluation of privacy filters[C]// SPIE Optical Engineering+Applications. 2013:219-224.
- [62] SOHN H, LEE D, NEVE W D, et al. An objective and subjective evaluation of content-based privacy protection of face images in video surveillance systems using JPEG XR[M]// Effective Surveillance for Homeland Security: Balancing Technology and Social issues. Boca Raton: CRC Press, Taylor & Francis, 2013: 111-140.
- [63] ERDÉLYI Á, WINKLER T, RINNER B. Privacy protection vs. utility in visual data-An objective evaluation framework[J]. Multimedia Tools and Applications, 2018, 77(2):2285-2312.



JIN Hua, born in 1977, Ph.D, associate professor. His main research interests include privacy protection and information security.

(责任编辑:喻黎)