doi:10.3969/j.issn.1000-436x.2013.08.020

视频隐私保护技术综述

佟玲玲，李扬曦，黄文廷
（国家计算机网络应急技术处理协调中心，北京 100029）

摘 要：互联网的快速发展和各类视频应用的日益普及，使视频个人隐私保护得到广泛关注。如何在保证视频应用的同时使隐私信息不被泄露是目前亟待研究和解决的热点问题。针对这些问题从视频隐私保护技术的研究现状进行综述，从隐私提取、隐私区域保护及访问权限控制 3 个方面进行概括、比较和分析。此外，对与视频隐私保护相关的一些问题，如隐私的定义、感知安全性评价等方面进行了讨论。最后总结了视频隐私保护技术面临的挑战，并对其发展趋势进行展望。
关键词：数据隐藏；隐私保护；隐私区域提取；视频加密
中图分类号：TP37 **文献标识码**：A **文章编号**：1000-436X(2013)08-0154-07

Review on video privacy protection

TONG Ling-ling, LI Yang-xi, HUANG Wen-ting
(National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China)

Abstract: With the rapid development of the Internet and the tremendous proliferation of video applications, video privacy protection has garnered significant attention nowadays. It is a key problem to protect privacy while ensuring normal application. A survey of video privacy protection technologies was presented, and summary, comparison and analysis were mainly in three aspects: privacy extraction, privacy protection and access control. Moreover, some distinctive issues that correlate to privacy protection in video surveillance, such as privacy definition and perceptive security evaluation were also addressed. Finally, challenges and perspectives of video privacy protection technology were discussed.
Key words: data hiding; privacy protection; privacy region extraction; video encryption

1 引言

近年来，随着人们对公共安全的不断关注，视频监控系统日益普及，但长期的摄像监控使个人隐私受到极大威胁。此外，随着网络性能的持续提高和多媒体应用的快速发展，网络空间中的私有视频被曝光更是经常发生。

这些泄密事件，不仅对当事人的生活造成重大影响，有些还与国家的政治、经济及社会稳定等方面密切相关。因此，如何保证视频个人隐私不被泄露是目前亟待研究和解决的热点问题。

视频隐私保护技术以其较高的学术价值和巨大的应用潜力，得到了研究者的极大关注。目前，各国学者相继开展了这方向的研究，取得了一定的研究成果。鉴于国内外尚未有详细而全面介绍视频隐私保护技术研究成果的综述论文，笔者通过跟踪研究，总结了目前该领域的研究成果及存在的问题，并对其发展进行展望。

2 相关研究

视频隐私保护技术早期研究动力来源于监控视频隐私保护这一应用需求。通过对视频中能够直接或间接识别个人身份的隐私区域（如运动人体、人脸等）进行保护，而其他区域仍对所有用户保持可见，实现了公共安全和个人隐私的良好平衡。

2003 年，IBM 的研究者在其构建的 PrivacyCam

收稿日期：2013-05-04；**修回日期**：2013-06-28
基金项目：新一代宽带无线移动通信网科技重大专项基金资助项目（2011x03002-005-01）
Foundation Item: Science and Technology Major Projects of New Generation of Broadband Wireless Mobile Communication Network (2011x03002-005-01)

系统中最早提出了视频隐私保护的思想[1]。随后，国内外卡内基梅隆大学、加州大学、大阪大学、清华大学、中国科学院计算所等一批著名研究机构的学者相继开展了这一方向的研究。近几年来，在著名的国际会议(如 IEEE ICIP，IEEE ICME，IEEE CVPR，ACM Multimedia)，及国际权威杂志 (如《IEEE Signal Processing Magazine》《IEEE transactions on Circuits and Systems for Video Technology》《IEEE transactions on Knowledge and Data Engineering》) 上发表的相关文章数量也显著增加。在 2011 年，一些国际权威杂志（如《Multimedia System Journal》[2]《Journal of Multimedia》[3]《Journal of Visual Communication and Image Representation》[4]）分别设立了视频隐私保护相关的专刊。可见，视频隐私保护技术是一个新兴而活跃的研究领域。

3　视频隐私保护技术

现有视频隐私保护方案主要从以下 3 个方面进行区分：如何提取隐私区域、采用何方法保护隐私区域及如何针对不同用户设定隐私数据访问权限。

3.1　隐私区域提取

快速准确的隐私区域提取是视频隐私保护的前提。不同的视频隐私保护方案通常依据其应用场景选择不同的提取方法。现存的隐私区域提取方法主要可以分为以下 3 类：运动物体提取、人脸检测及基于辅助信息的方法。

3.1.1　运动物体提取

运动物体通常是视频中的主体，包含着视频的关键信息，因此，多数视频隐私保护方案选择运动区域进行保护[5,6]。对运动物体进行保护能够很好地满足视频监控等以运动物体为主的视频应用。视频隐私保护领域常用的运动物体提取主要采用静止背景中的运动前景检测及跟踪方法。选择比较简单的方法主要出于对应用需求及速度方面的考虑。视频运动物体提取是一项非常热门的研究课题，近年来取得了许多研究成果[7,8]。

3.1.2　人脸检测

除运动物体外，人脸也是视频中的重要区域，在身份识别中起着重要作用，因此一些视频隐私保护方案通过保护人脸区域实现隐私保护[9,10]。人脸区域的保护可用于视频会议等以人脸为主体的视频应用中。用于视频隐私保护的典型人脸检测方法包括：基于头—肩分析的人脸检测方法[10]，基于类 Haar 特征的人脸检测[11]及基于特征脸的人脸检测[12]等。有时采用人脸检测与跟踪[13]相结合的方法提高检测的准确度。人脸检测与识别也是一项广受关注的热门课题，研究成果不胜枚举[14]。

基于辅助信息的提取方法利用人为设置的外部辅助信息进行隐私区域的提取。这类方法能够按不同应用的需求自适应地选取保护区域。提取对象仍然以运动物体和人脸区域为主。用于提取的辅助信息包括人眼可见及不可见信息。

1) 基于可见信息的提取

该类方法假设需要保护的隐私区域具有某种视觉特征。文献[15]设定需要保护的人穿有特定颜色的衣服。利用颜色特征进一步提取出相关的人脸区域，并对这些人脸区域进行保护（如图 1 所示）。类似地，文献[16]中设定需要保护的人衣服上有特定颜色的小标签，通过颜色分类器检测出需要保护的个体。基于颜色信息的提取方法虽然能够快速提取出隐私区域，但是这种方法容易受外界噪声的干扰，如背景中有同样颜色时，会造成误检。

图 1　基于标记的人脸区域保护

2) 基于不可见信息的提取

非视觉模态信息同样可用来辅助隐私区域提取，但该类方法通常需要额外的硬件设备辅助。文献[17]采用基于人眼的虹膜识别方法实现对特定人群的信息保护。文献[18]则通过在一个概率框架中融合了颜色、位置、声音等多种信息来提取运动人体进行保护。文献[19]采用视频、红外线、声音等同时用于提取需要保护的运动物体。有时，全球定位系统（GPS）[20]及射频识别（RFID）系统[21]也用于辅助检测。

通过以上分析可以看出，在视频隐私保护中，隐私区域提取主要根据不同的应用场景选择不同的方法。多数方案采用现存的运动物体或人脸提取方法确定保护区域，有些则基于假设条件，利用辅助信息进行提取。提取的对象主要包括运动物体和人脸区域。

3.2 隐私区域保护

提取出隐私区域后，需要采取措施将这些区域保护起来。本节将对现有的视频隐私保护方法进行分析总结。

由于视频通常经过压缩编码再进行存储和传输，因此，本节将视频隐私区域保护方法依据其在编码过程中所处的位置分为 3 类：编码前保护、与编码相结合的保护及基于数据隐藏[22]的保护。其中，基于数据隐藏的方法可看作前 2 种方法的结合，即隐私数据在编码前被加密，之后这些数据在编码过程中被嵌入到保护后的视频中。由于在视频压缩编码后再对隐私区域进行保护（图 2 虚线部分）需要重新解码来确定隐私区域的位置，效率较低，因此这类方法并未使用。

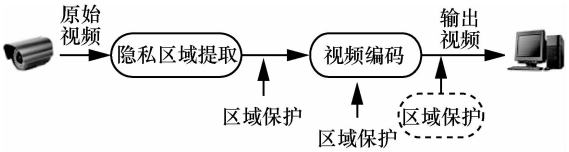


图 2 隐私区域保护方法分类

3.2.1 编码前保护

这类保护方法在像素域数据上对隐私区域进行保护，视频在传输给编码器进行压缩编码之前需要保护的信息已经被去除。

由于其简单和直观性，这类方法在早期的视频隐私保护中广泛使用。使用这种方法保护的视频，隐私区域的数据通常不可恢复的。

这类方法主要可以分为以下 3 类。

1) 数据替换

数据替换方法通过将需要保护的数据用其他数据替代，实现隐私区域保护。有很多研究成果采用这种隐私保护方法。可以通过保持物体结构特性但去除其外观[6]，人脸的替换[11]、打马赛克或者模糊[15, 23, 24]，对像素域数据进行加密[25, 26]等方法实现数据替换。图 3 列出了采用上述方法进行隐私保护的例子，其中左侧面为原始图像，右侧面为相应的隐私保护结果。

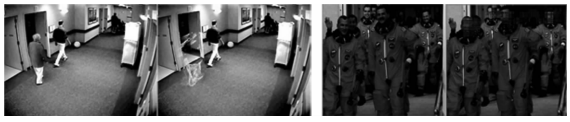
2) 视频多重拷贝

该方法通过向具有不同权限的用户提供包含视频中不同内容的拷贝实现隐私保护。这种方法在 IBM 实现的 PrivacyCam 系统中被提出[1]。若要得到视频内容的多份拷贝，在这个系统必须包含一个视频内容分析子系统。该子系统首先对视频内容进行详细分析，提取出视频的关键因素，如视频的时间、地点及主要人物等。这些信息可单独形成原始视频的一份拷贝，也可以几个结合作为一份新的拷贝进行存储和传输。

视频的多重拷贝能够实现精细粒度的访问权限控制，但这种方法受限于视频内容分析子系统的性能，而且非常耗时。此外，保存不同的视频拷贝需要较大的存储空间。

(a) 黑框 (b) 马赛克

(c) 人脸替换 (d) 指数时空域模糊



(e) 去除外观保持结构 (f) 像素域加密

图 3 数据替换典型方法

3) 数据分割

该方法将视频图像分割成多份随机数据。每份数据都无法单独辨识原始图像，只有将所有数据合在一起才能够恢复原始视频[27]。数据分割后，同一视频的不同分割被传送到不同终端分布式存储。

这种方法实现了安全的分布式处理和存储，当需要时可恢复原始视频。虽然这种方法能够提供较高的安全性，但整个视频场景被破坏，无法满足应用需求。同时需要较多的处理器及存储空间。

3.2.2 与编码结合的保护

与编码结合的保护方法通过选择视频编码过程中的关键数据或关键步骤进行加密，实现视频隐私保护。

图 4 为一个典型的视频编码框架。根据隐私区域加密的位置，与编码结合的保护方法主要可以分为 5 类：变换加密、帧内预测模式加密、运动矢量加密、变换系数加密及熵编码过程加密。

1) 变换加密

在视频编码过程中，预测得到的残差系数经过变换编码，实现数据的进一步压缩。变换加密方法

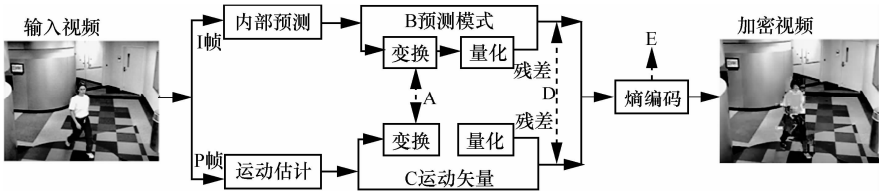


图 4　与视频编码相结合的保护方法分类

通过改变标准变换中的角度实现加密[28, 29]。变换加密需要事先设计候选的变换方法，复杂度较高。同时，由于所采用的变换与原变换要具有相似或更优的编码效率，这种加密方法对视频数据的改变较小，使得加密视频混乱程度不高，视觉安全性较差。

2) 帧内预测模式加密

帧内预测模式对帧内编码图像非常重要。文献[30]中最早提出了帧内预测模式的加密方法。这种加密方法实现简单，加密前后码长不变，但其安全性主要取决于加密的定长随机序列。为了提高安全性，文献[31]使用二维混沌序列改进上述方法。帧内预测模式加密仅适用于帧内编码图像，帧间编码图像则通过参考加密的图像依靠误差传播实现加密。可见这种方法的安全性不高，通常与其他加密方法相结合来提高安全性[32]。

3) 运动矢量加密

运动矢量表示视频的运动信息，对视频重建十分重要，文献[33]仅利用运动矢量从像素加密的视频中恢复出较低分辨率的视频，证明了运动矢量的重要性。随后研究者提出了多种运动矢量加密方法，主要包括运动矢量差符号位加密[33, 34]及运动矢量幅值和方向的加密[35~37]。由于该类算法没有加密亮度和纹理信息，其安全性较低，因此，运动信息加密通常与其他方法结合以提高安全性。

4) 变换系数加密

视频经变换编码后，主要信息集中在变换系数中，对其加密能够很好地保护原始视频。变换系数加密方法主要包括系数位置的置乱[38, 39]，系数幅值直接加密[40]和系数符号位加密等方法[41]。

5) 熵编码过程加密

熵编码是视频压缩编码的重要部分之一，它利用输入信号的统计特性实现数据压缩。基于熵编码的视频加密方法主要分为熵编码模型参数加密[42]和熵编码过程的关键数据[43]加密。

6) 误差漂移

与编码相结合的视频隐私保护中存在的一个关键问题是非授权解码端的误差漂移。误差漂移是由于编码端和非授权解码端参考数据不一致引起的非加密区域的解码误差[41]（如图 5 所示）。如不采取措施，误差漂移将使视频场景无法辨识。

图 5　视频局部区域加密中的误差漂移

为了抑制误差漂移，文献[41]、文献[44]和文献[45]分别提出了相应的方法。但这类方法大都比较简单，由于禁止了相关宏块的数据参考，编码效率显著降低。文献[46]中，作者提出了完整的误差漂移抑制方法，充分利用可预测的数据提高编码效率。

综上所述，在视频编码过程中，无论在变换域还是熵编码域，残差变换系数、帧内预测模式和运动矢量对于视频的重建十分重要，因此现有的与编码结合的保护方法多选择这 3 种关键数据进行加密。由于视频在压缩域的数据量减小，与编码结合的保护方法通常安全性不高，也有一些方案采用多种元素联合加密的方式来提高安全性。

3.2.3　基于数据隐藏的方法

该方法指隐私区域数据不仅被保护起来，而且被（采用数据隐藏的方法）嵌入到保护后的视频中。通常，数据隐藏需要与精确的物体替换或者图像修补相结合以保证视频图像不失真。当需要原始视频时，这些数据可以完全恢复。

Li G 等人提出基于离散小波变换的隐私区域保护方法[47]。该方法采用 DWT 变换生成隐私区域的高分辨率图像及低分辨率图像。然后通过数据隐藏方法将高分辨率细节信息嵌入到原始视频中。为了使保护后的视频仍保持原始视频的可用性，文献[48]提出了一个保护监控视频中人脸区域的框架。在这个框架中，首先提取人脸区域，并将这些区域信息通过数据隐藏的方法嵌入到主图像中。然后用一个

新的人脸替换原始人脸区域。这样在保证加密视频可用性的同时使个人信息得到保护。

文献[49]考虑了整个人体运动区域的保护，提出了基于视觉模型（perceptual-model-based）的压缩域数据隐藏方法，将保护区域中的数据全部嵌入原始视频。该方法由于需要将大量数据嵌入到原始视频当中，编码效率显著降低。

为了提高编码效率，文献[19]提出了改进的视频隐私区域保护系统，采用一种基于率失真优化的数据隐藏方法将加密区域数据嵌入到原始视频中。为了保证修改后视频的自然外观，该系统采用了一种基于图像修补（image inpainting）的方法[54]将去掉的加密区域用背景数据进行替换。

由于攻击者不知道隐藏数据的存在，因此基于数据隐藏的方法通常具有较高的安全性。但这种方法复杂度较高，图像修补和数据隐藏的过程都很耗时。此外，这种方法最大的挑战在于如何嵌入大量的视频数据但却保持较高的编码效率。

3.3 隐私访问权限控制

当恢复隐私数据时，需要有相应的访问权限控制机制，使得有特定权限的用户才可访问隐私数据。虽然研究者进行了相关的研究[6,21,50]，提出了如基于第三方的数字权限管理系统等方法，但在大多数隐私保护系统中这一问题并未被提及。

实际上，数据的访问权限控制对于视频隐私保护系统至关重要。任何授权密钥的非法使用将使整个系统毫无意义。因此，灵活的隐私权限控制是处理复杂的隐私策略时不可缺少的部分。

3.4 典型方案比较

为了能对现有的视频隐私保护方案有整体的了解，本节从系统的角度进行总结。如表 1 所示，现有的视频隐私保护方案主要针对特定的应用场景，采用不同的隐私区域提取和保护方法。其中，隐私区域提取主要利用已有的方法提取运动物体或人脸区域进行保护。有些方案则针对特定的应用需求，采用一定的辅助信息进行区域的提取。有些方案甚至不考虑隐私区域提取，在假设其已知的情况下，重点研究对这些区域进行保护的方法。对于隐私区域保护方法的研究，开始主要集中在编码前的保护方法。这种方法简单易于实现，但是采用这种方法保护后的视频多无法恢复原始信息。在编码前直接对像素域数据进行加密，由于视频数据量大，加密效率较低。而基于数据隐藏的方法通常计算复杂度高，对编码效率影响大，仅适用于安全性要求较高的场景。与编码相结合的保护方法以其实现简单、加密效率高、保持加密视频格式兼容性等特点，得到了广泛关注。这种方法通过选择视频编码过程中与隐私区域相关的变换系数、帧内预测模式及运动矢量等关键数据或者步骤进行加密。

4 视频隐私保护技术的难点与趋势

本文从不同角度对视频隐私保护方法进行了系统综述。

视频隐私保护技术的发展经历了从简单的数据替换，到与视频编码相结合的保护，再到基于数据隐藏的保护；从对人脸的保护到人整个身体的保护；

表 1 典型的视频隐私保护方案

文献	隐私区域提取	隐私区域保护	应用场景
[6]	融合 RFID 信息的简单背景运动物体检测	编码前保护：数据替换	有简单背景的室内环境，保护特定人物信息
[9]	基于 PCA 的人脸识别方法[16]	编码前保护：数据替换	使用人脸识别软件进行面部图像识别
[15]	基于辅助信息的人脸检测	编码前保护：数据替换	复杂场景中的特定人物保护
[25, 26]	假设区域已知	编码前保护：编码前加密	与编码标准无关的场景
[11]	人脸及运动区域检测	编码前保护：编码前加密	室内及室外视频监控系统
[10]	运动检测及跟踪	编码前保护：去除外观保持结构	养老院，保护特定人物但保持其行为可见
[1]	假设区域已知	编码前保护：数据多重拷贝	视频监控系统
[41,53]	假设区域已知	与编码结合的保护：变换系数加密	视频监控系统
[5]	假设区域已知	与编码结合的保护：熵编码加密	需要对物体形状及纹理信息同时进行保护的场景
[45]	运动物体及人脸检测	与编码结合的保护：熵编码加密	网络多媒体应用
[19]	基于辅助信息的运动物体检测	数据隐藏：基于物体的图像修补和数据隐藏	实验室环境下的多摄像头系统
[49]	人脸检测	数据隐藏：人脸替换和数据隐藏	视频监控系统

从简单的隐私数据替换到保护隐私的同时保证视频场景的可理解性这样一个过程。虽然这一领域的研究取得了显著的进步，但仍有较多值得探讨和研究的领域，具体包括如下三方面。

1) 如何在实际应用场景中准确提取隐私区域？首先隐私的定义并不明确。在不同的应用场景下其含义各不相同。如果显性和隐性的身份泄露渠道同时考虑，如位置、阳光这类隐性信息很难提取。现有的多数工作将隐私定义为能够反映个人身份的信息。更多的隐性信息并未得到关注。即便仅考虑显著信息，不断变化的光照条件、对准确率的较高要求都使隐私区域的准确提取面临巨大挑战。

2) 如何满足实时应用的需求？现有的大多数隐私保护方案主要关注安全性和视觉质量，很少关注计算复杂度。而在实际应用中，实时性是必须的。因此，需要研究具有低复杂度的隐私保护方法，特别是在资源有限的应用中。

3）如何评价各类隐私保护方法的有效性？目前还没有公认的评价指标。多数系统采用自定义的标准来评价不同的方法。因此亟需研究有效的隐私保护评价指标，评价不同方法的有效性。如隐私保护视频的视觉安全性是衡量隐私保护方法的一项重要指标。文献[51]和文献[52]进行了初步的研究，但仍有许多工作需要开展，如建立隐私保护视频数据库、进行主观的视觉安全性评价等。

视频隐私保护是一个全新的研究领域，也是一个真正的跨学科课题，需要隐私保护倡导者、法律专家、技术专家等各方面的努力。目前隐私保护系统的实际应用较少。大多数解决方案都限定在实验室环境。能够满足实际应用的视频隐私保护系统仍然是今后研究的目标。然而，即将出现的强大视频分析工具及政府、公众等多方面的关注，将使这一领域前途光明。

5　结束语

视频隐私保护是一个新兴而活跃的研究领域，对于保护个人隐私安全，促进相关应用发展具有重要的意义。本文总结了视频隐私保护技术的研究进展，并对其面临的问题进行归纳和分析，希望促进我国该领域及其相关研究发展。

参考文献：

[1] SENIOR A, PANKANTI S, *et al*. Blinkering Surveillance: Enabling Video Privacy Through Computer Vision[R]. IBM Technical Paper, RC22886 (W0308-109), 2003.

[2] Special issue on privacy-aware multimedia surveillance systems[EB/OL]. http://link.springer.com/article/10.1007%2Fs00530-011-0251-z

[3] Special issue on multimedia contents security in social networks applications[EB/OL]. http://www.academypublisher.com/jmm/si/jmmsi_mcs.html.

[4] Special issue on recent advances on analysis and processing for distributed video systems[EB/OL]. http://dl.acm.org/citation.cfm?id=1942350.

[5] MARTIN K, PLATANIOTIS K N. Privacy protected surveillance using secure visual object coding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2008, 18(8):1152-1162.

[6] WICKRAMASURI J, DATT M, *et al*. Privacy protecting data collection in media spaces[A]. Proceedings of the 12th annual ACM international conference on Multimedia[C]. ACM, 2004. 48-55.

[7] STAUFFER C, GRIMSON W E L. Adaptive background mixture models for real-time tracking[A]. IEEE Computer Society Conference on Computer Vision and Pattern Recognition[C]. 1999.

[8] STAUFFER C, GRIMSON W L. Learning patterns of activity using real-time tracking[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(8):747-757.

[9] NEWTON E, SWEENEY L, MAIN B. Preserving privacy by de-identifying face images[J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(2):232-243.

[10] CHEN D, CHANG Y, YAN R, *et al*. Tools for protecting the privacy of specific individuals in video[J]. EURASIP Journal on Advances in Signal Processing, 2007, (2007):1-9.

[11] BOULT E. Pico: privacy through invertible cryptographic obscuration[A]. Computer Vision for Interactive and Intelligent Environment[C]. 2005. 27-38.

[12] TURK M, PENTLAND A. Eigenfaces for recognition[J]. Journal of Cognitive Neuroscience, 1991, 3(1):71-86.

[13] YILMAZ A, JAVED O, SHAH M. Object tracking: a survey[J]. Acm Computing Surveys, 2006, 38(4):13-18.

[14] YANG M, KRIEGMAN D, AHUJA N. Detecting faces in images: a survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(1): 34-58.

[15] SCHIFF J *et al*. Respectful cameras: detecting visual markers in real-time to address privacy concerns[A]. Protecting Privacy in Video Surveillance[C]. London Springer, 2009.

[16] ZHAO J, CHEUNG S C. Multi-camera surveillance with visual tagging and generic camera placement[A]. ACM/IEEE Int Conf on Distributed Smart Cameras[C]. 2007. 259-266.

[17] LUO Y, *et al*. Anonymous subject identification in privacy-aware video surveillance[A]., IEEE International Conference on Multimedia and Expo (ICME)[C]. 2010. 83-88.

[18] MEGHERBI N, *et al*. Joint audio-video people tracking using belief theory[A]. IEEE Int Conf on Advanced Video and Signal Based Surveillance[C]. 2005. 135-140.

[19] KUMAR P, MITTAL A. A multimodal audio visible and infrared surveillance system (maviss)[A]. IEEE Int Conf of Intelligent Sensing and Information Processing[C]. 2005. 151-156.

[20] SHAKSHUKI E, WANG Y. Using agent-based approach to tracking moving objects[A]. 17th International Conference on 2003 Advanced Information Networking and Applications[C]. 2003. 578-581.

[21] CHEUNG S C, *et al*. Protecting and managing privacy information in video surveillance systems[A]. Protecting Privacy in Video Surveillance[C]. 2009.11-33.

[22] SOLANKI K, *et al*. High-volume data hiding in images: introducing perceptual criteria into quantization based embedding[A]. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)[C]. 2002.3485-3488.

[23] AGRAWAL P, NARAYANAN P J. Person de-identification in vid-

eos[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2011, 21(3): 299-310.
[24] KITAHARA I, *et al*. Stealth vision for protecting privacy[A]. Proceedings of the 17th International Conference on Pattern Recognition[C]. 2004. 404-407.
[25] CARRILLO P, KALVA H, MAGLIVERAS S. Compression independent object encryption for ensuring privacy in video surveillance[A]. IEEE International Conference on Multimedia and Expo[C]. 2008. 273-276.
[26] CARRILLO P, KALVA H, MAGLIVERAS S. Compression independent reversible encryption for privacy in video surveillance[J]. EURASIP Journal on Information Security, 2009, (2009):1-13.
[27] UPMANYU M, *et al*. Efficient privacy preserving video surveillance[A]. IEEE 12th International Conference on Computer Vision[C]. 2009. 1639-1646.
[28] YEUNG S, ZHU S, ZENG B. Partial video encryption based on alternative integer transforms[A]. Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS)[C]. 2010. 933-936.
[29] YEUNG S, ZHU S, ZENG B. Partial video encryption based on alternating transforms[J] IEEE Signal Processing Letters, 2009, 16(10): 893-896.
[30] AHN J, SHIM H J, JEON B, *et al*. Digital video scrambling method using intra prediction mode[A]. Advances in Multimedia Information Processing-PCM 2004[C]. Springer Berlin Heidelberg, 2005. 386-393.
[31] 蒋建国, 李援, 梁立伟. H. 264 视频加密算法的研究及改进[J]. 电子学报, 2007, 35(9): 1724-1727.
JIANG J G, LI Y, LIANG L W. Research and improvement of the video encryption algorithm for H.264[J]. Chinese Journal of Electronics, 2007, 35(9):1724-1727.
[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] LIU Z, LI X. Motion vector encryption in multimedia streaming[A]. Proceedings 10th International Multimedia Modelling Conference[C]. 2004. 64-71.
[34] SU P, HSU C, WU C. A practical design of content protection for H. 264/AVC compressed videos by selective encryption and fingerprinting[J]. Multimedia Tools and Applications, 2011, 52(2/3): 529-549.
[35] LI S, *et al*. On the design of perceptual MPEG-video encryption algorithms[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2007, 17(2): 214-223.
[36] THOMAS N. A novel secure H. 264 transcoder using selective encryption[A]. International Conference on Image Processing. IEEE[C]. 2007. 85-88.
[37] LIU Y, YUAN C, ZHONG Y. A new digital rights management system in mobile applications using H. 264 encryption[A]. The 9th International Conference on Advanced Communication Technology[C]. 2007. 583-586.
[38] TOSUN A, FENG W. Efficient multi-layer coding and encryption of MPEG video streams[A]. IEEE International Conference on Multimedia and Expo[C]. 2000. 119-122.
[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. Low complexity controllable scrambler/descrambler for H.264/AVC in compressed domain[A]. Proceedings of the 14th annual ACM international conference on Multimedia[C]. 2006. 93-96.
[41] DUFAUX F, EBRAHIMI T. Scrambling for privacy protection in video surveillance systems[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2008, 18(8):1168-1174.
[42] XIE D, KUO C. Enhanced multiple Huffman table (MHT) encryption scheme using key hopping[A]. Proceedings of the International Symposium on Circuits and Systems[C]. 2004. 568-571.
[43] 包先雨, 蒋建国, 袁炜等. H.264/AVC 标准中基于 CABAC 的数字视频加密研究[J]. 通信学报, 2007, 28(6): 24-29.
BAO X Y, JIANG J G, YUAN W, *et al*. Study of CABAC-based digital video encryption in the H.264/AVC standard[J]. Journal on Communications, 2007, 28(6):24-29.
[44] DUFAUX F, EBRAHIMI T. H.264/AVC video scrambling for privacy protection[A]. 15th IEEE International Conference on Image Processing[C]. 2008. 1688-1691.
[45] 于俊清, 刘青, 何云峰. 基于感兴趣区域的 H.264 视频加密算法[J]. 计算机学报, 2010, 33(5):945-953.
YU J Q, LIU Q, HE Y F. H.264 Video encryption algorithm based on region of interest[J]. Chinese Journal of Computers, 2010, 33(5): 945-953.
[46] DAI F, TONG L, ZHANG Y, *et al*. Restricted H. 264/AVC video coding for privacy protected video scrambling[J]. Journal of Visual Communication and Image Representation, 2011, 22(6):479-490.
[47] LI G, ITO Y, YU X, *et al*. A discrete wavelet transform based recoverable image processing for privacy protection[A]. Proceedings of the 15th IEEE International Conference on Image Processing[C]. 2008. 1372-1375.
[48] YU X, BABAGUCHI N. Privacy preserving: hiding a face in a face[A]. Computer Vision–ACCV 2007[C]. Springer Berlin Heidelberg, 2007. 651-661.
[49] ZHANG W, CHEUNG S C. CHEN M. Hiding privacy information in video surveillance system[A]. Proceedings of the 12th IEEE International Conference on Image Processing[C]. 2005. 868-871.
[50] LIOUDAKIS G, *et al*. A middleware architecture for privacy protection[J]. Computer Networks, 2007, 51(16):4679-4696.
[51] SUN J, XU Z, LIU J, *et al*. An objective visual security assessment for cipher-images based on local entropy[J]. Multimedia Tools and Applications, 2011, 53(1):75-95.
[52] TONG L L, DAI F, ZHANG Y D, *et al*. Visual security evaluation for video encryption[A]. Proceedings of the International Conference on Multimedia[C]. 2010. 835-838.
[53] HOSIK S, NEVE W, YONG R. Privacy protection in video surveillance systems: analysis of subband-adaptive scrambling in JPEG XR[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2011, 21(2): 170-177.
[54] VENKATESH M, CHEUNG S, ZHAO J. Efficient object-based video inpainting[J]. Pattern Recognition Letters, 2009, 30(2): 168-179.

作者简介：

佟玲玲（1985-），女，辽宁阜新人，国家计算机网络应急技术处理协调中心工程师，主要研究方向为多媒体内容分析与安全，视频编解码等。

李扬曦（1982-），男， 甘肃兰州人，国家计算机网络应急技术处理协调中心工程师，主要研究方向为多媒体检索、机器学习。

黄文廷[通信作者]（1982-），男，江苏徐州人，国家计算机网络应急技术处理协调中心工程师，主要研究方向为物联网技术及安全、视频编解码。E-mail: hwt@cert.org.cn。