去身份识别技术综述

车辚辚，韩东升
（华北电力大学 电气与电子工程学院，河北 保定 071003）

摘　要：首先对去身份识别技术的应用背景和影响因素进行了概括；然后对以影响因素为基础的去身份识别研究成果进行了全面论述，并对去身份识别算法的健壮性要求进行了讨论；最后归纳了当前研究存在的问题与挑战。

关键词：去身份识别；行为识别；隐私保护；视频监控
中图分类号：TP391.4　　**文献标志码**：A　　**文章编号**：1001-3695(2013)02-0341-05
doi:10.3969/j.issn.1001-3695.2013.02.005

Review of person de-identification techniques

CHE Lin-lin, HAN Dong-sheng
(*School of Electrical & Electronic Engineering*, *North China Electric Power University*, *Baoding Hebei* 071003, *China*)

Abstract: This paper generalized the application background and influencing factors of person de-identification at first. Subsequently, it reviewed many studies of person de-identification based on influencing factors in detail. And it discussed robustness of the person de-identification algorithm. Finally, it concluded some research issues and challenges in person de-identification.

Key words: person de-identification; action recognition; privacy protection; video surveillance

0　引言

随着计算机技术和电子技术的不断发展，人类生活的自动化水平不断提升，在以智慧地球为背景的物联网技术不断推进的情况下，可供监控和获取的信息越来越多。如今，无论你是出入于商业楼宇，还是公共场所（如医院、车站、学校等），甚至是在自己居住的小区内行走，你的信息都可能通过物联网设备被获得[1]。有数据显示，大规模的监控系统在控制犯罪方面发挥了强大的积极作用[2]。然而，这些信息在为人类提供便捷服务和全方位保护的同时也产生了另外一些问题，视频信息中的个人隐私保护就是其中一个需要重点被关注的问题[3]。因此，在视频信息中研究去身份识别技术是十分必要的。该技术不但可以提供有效的视频信息，还可以保护个人信息不被泄露。

去身份识别技术是在视频及图像数据中去除可以确定前景身份的相关信息，但是要保留足够的信息去判断前景的动作行为。图像处理研究中的去身份识别技术是在模糊化身份特征的基础上进行动作识别和行为理解。去身份识别的过程中，只关注视频监控系统中四个 W 因素中的 when、where 和 what 这三个因素，而需要加密或模糊化 who 这个因素。

基于现实问题的需要，本文对新近发展起来的去身份识别技术进行以下几方面的论述，从而为未来的研究阐明方向：

a）去身份识别技术的应用背景。对于不同视频数据资料的用途不同，因此对于去身份识别技术的要求也不同，应采取相应的方法。

b）影响去身份识别的因素。这其中主要以生物信息因素为主。

c）对以影响因素为基础的去身份识别成果进行全面论述。

d）分析了存在的问题及挑战。

由于去身份识别技术刚刚起步，并且技术有许多不成熟的地方。所以本文对去身份识别技术的介绍和讨论都只是略述皮毛，希望对今后的研究有些许指引作用。

1　应用背景

去身份识别技术在个人信息保护领域有着广泛的应用背景。近几年由于公共安全的需要，生物识别和视频监控方面的需求迅速增加。除此之外，随着互联网技术的迅猛发展，网络上的共享信息也大量出现。在这些公开的信息中，隐私保护就成为了人们普遍关注和担忧的问题[4]。

早期的关于隐私保护的讨论起源于闭路电视系统（CCTV）。美国公民自由协会（ACLU）描述了关于闭路电视系统五种被滥用的类型：以犯罪为目的、以慈善为目的、以个人利益为目的、被冠以歧视性标签、窥淫癖者。视频监控系统在给人类带来便利的同时也存在着潜在的巨大风险，而风险被重视的程度远远低于前者，因此使两者在发展过程中出现了严重的失衡。不仅是 ACLU，还有其他组织也同样提出了以上的问题。Senior 等人[5]对视频系统中隐私保护的重要性进行了全面论述，并对可能进行的保护措施进行了罗列。随着视频数据中隐私信息泄露事件的日益增多，个人隐私保护问题受到了更

收稿日期：2012-07-03；**修回日期**：2012-08-13

作者简介：车辚辚（1981-），女，河北保定人，工程师，硕士，主要研究方向为数字图像处理、通信与信息系统（linlin.c@sohu.com）；韩东升（1980-），男，黑龙江齐齐哈尔人，讲师，博士，主要研究方向为无线通信、数字图像处理.

广泛的关注[6,7]。因此,对于视频及图像数据的去身份识别技术显得尤为重要,并且越来越多的学者开始对这个领域进行深层次的研究。

随着计算机和互联网的不断发展及创新,可能需要用到去身份识别的数据大体可以分为如下三类[8]:a)视频及图像数据中的人物信息并不重要,人物信息可以被永久删除;b)在公开数据中的人物信息进行去身份识别,但对于存档信息需要可以还原其中的人物信息;c)对于信息中的大部分人物信息可以公开,只对提出保护的个别人物需要进行去身份识别。

被放置于公共场合的网络摄像头记录的数据或者分享在网络上的图像信息等都可属于第一类情况。例如,谷歌街景中包含的私人信息(如汽车牌照、行人等)是偶然被拍摄的,并不是地图所关心的信息,这一部分内容是可以被永久删除而并不影响地图的实用效果。第二类情况主要包括用于公共场所(医院、学校、车站等)监控的图像信息。在这类情况中的图像信息主要是用于防范公共场所的危险行为及状况,而在监控端并不关注每个人的个人信息(如脸部、步态等),只需要在信息存档时提供个人信息即可。因此,在监控端的图像信息中,需要采取去身份识别技术来对个人信息进行保护。基于以上情况提出了可还原的去身份识别技术。与第一种情况不同之处在于,前者的去识别是不可逆的,而后者可以完全还原原始信息。第三类情况主要针对半开放私人场所,如办公室、私人会所等。出入这些场所的人大多是有预约的,对于该场所获得的个人影像资料应该不是需要保护的,而对于提出特殊需求的个人可对其影像资料按照其要求进行去身份识别处理。

2 影响因素

为了实现视频及图像信息的去身份识别,以及更好地分析去身份识别算法的效果,必须全面考虑影响其效果的因素,从而采取相应的措施加以克服。影响去身份识别的因素主要是人的生物信息,其中包括脸、指纹、虹膜、外形轮廓、步态、声音等信息。

基于生物信息的特征大部分都是与视频识别中的特征相对应的。也就是说去身份识别算法的应用可以使识别算法的特征失效,即去身份识别以后的数据无法通过自动识别算法进行身份识别,但是仍然可以判断其行为。因此,本文主要对基于生物信息特征的去身份识别研究进行全面的论述。

3 研究现状

由于视频系统中隐私信息的重要性,相关研究人员已经提出了隐私信息保护系统的体系框架[9],但其中并没有给出具体实现[10,11]。个人隐私保护中关键的方面就是对视频和图像进行特殊处理,从而使得视频和图像中不再包含个人身份信息。在计算机视觉的图像处理中可以通过计算机语言编译实现对影像信息的改变[5]。图像处理中的检测和分割技术往往也经常被用于对感兴趣区域进行去识别处理[12,13]。对于特定的人群,射频识别标签等其他设备也被研究尝试应用于隐私保护[14,15]。除此之外,对于视频处理的过程中可以通过对数据流进行加密实现对整个信息的保护。以往通用的一些加密手段也是可以用于视频信息保护的[16,17],如水印的技术,但是由于其针对性差的特点,对于外形轮廓、步态等复杂生物信息很难达到去识别的效果。

对于数据安全而言,越靠近图像获取端进行去身份识别处理获得的数据就越安全[18]。因此有些学者对可以进行隐私保护的图像获取设备进行了研究[19~21]。Mrityunjay 等人[22]在 2011 年提出了一种镜头可伸缩、低成本、可实时保护隐私的去识别相机。他的主要贡献就在于开发了在视频捕获端通过变换进行隐私保护的硬件设备,并提出了一个适用于实时实现的去识别系统框架,如图 1 所示。该系统被应用于基于嵌入式平台系统的 OMAP4 Texas 仪器,在照相机端实现了实时保护隐私的效果。这种系统可以取代传统的监控摄像机,并且为未来的视频监控和公共隐私保护提供了硬件解决方案。

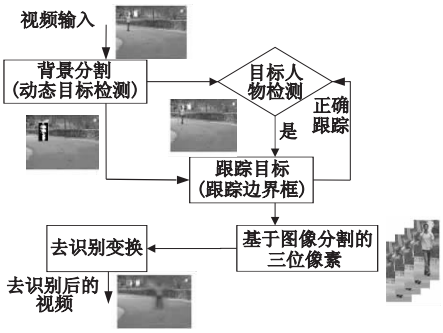

图1 去识别系统框架

去身份识别技术主要是对视频和图像中的人物信息进行特殊处理的过程。除了上述对于硬件的研究以外,对去身份识别算法进行研究可以使去识别效果更加完善。目前关于算法的研究基本上可以按照其影响因素来划分,以下将逐一介绍其研究现状。

3.1 基于脸部信息的去识别研究

目前,针对影响去身份识别因素中的生物信息有一些学者已经进行了一定的研究,并取得了阶段性的成果。其中,基于脸部信息的去身份识别研究开展得比较广泛,并且得到了良好的去身份识别效果。去身份识别技术的研究最早开始于对于脸部信息的去识别[23,24],这是由于脸部信息包含的个人信息是最直观的,也是最容易被辨别出来的[25]。基于脸部信息的去识别研究主要分成以下两个方面:基于原始图像像素改变或模糊化的脸部信息去识别、基于替换人脸模型的脸部信息去识别。这其中每个方面中的去识别技术又可分为可逆的和不可逆的两种情况。

基于原始图像像素改变或模糊化的脸部信息去识别,是在原始人脸数据上进行改变从而起到保护身份的作用。这种方法往往占用的资源比较少,不需要大规模的存储空间。Newton 等人[26]提出了 k-same 算法用于脸部信息的去识别。该算法在最邻近的 k 个脸部信息中得到平均值,用该值代替 k 个脸部信息。该算法可以在保存脸部特征的同时使脸部自动识别软件失效。Gross 等人在提出 k-same-select 算法[27]的基础上进一步探索了脸部的模型参数[28,29],通过设置不同的参数值来达到脸部信息的去识别效果,并且针对复杂的脸部模型的去识别,他们也提出了一种半监督学习的方法。为了适应各种环境,他们还提出了一种通用的图像去身份识别框架,在完成算法的同时对原有数据进行尽量小的变动[30]。Phillips 等人[31]从图像重建的角度对脸部信息的去识别进行了研究,其通过减少脸部信息重建过程中特征向量的方法,对脸部信息进行保

护。还有一些专门用于特定数据库的脸部信息的去识别算法,如自动模糊化脸部信息和车牌号码的算法被用于 Google Street View 数据库上[32]。以上介绍的去身份识别的方法都是不可逆的。还有一些学者使用加密技术对人脸信息进行保护,文献[33]提出了一种可逆的脸部信息去识别方法,该方法是通过水印技术对鲁棒哈希图像进行人脸信息去识别,因为水印技术是可还原的,所以该方法是可逆性的。

与在原始图像上进行变换不同,又有学者另辟蹊径,通过替换原有的脸部信息进行去识别。Bitouk 等人[34]提出一种人脸替换系统,该体系是在大规模人脸库中搜索与原有信息相似的脸图,对两幅图进行校准并在同一坐标系内进行替换。该系统完全自动化,并且其替换后的图像非常逼真。Ross 等人[35]在 2011 年提出了一种对人的生物特征(指纹、虹膜、脸)进行视觉加密的可能性。以脸部信息为例进行说明如图 2 所示,对一张人脸图在主机库里挑选两张公共人物的脸将其代替,并把两张图片分别存储于不同的两个数据库服务器内,这样的话只有在两张图片都被截获的时候,私人照片信息才会被泄露。通过两张公共人物的脸可以对原始图像进行重建。这个过程中,同一张私人面孔可以用公共人物的脸随机组合,所以其加密过程可以有多种可能的方案。利用 XM2VTS 和 IMM 人脸数据库证明了该算法的有效性和健壮性,并且该方法对其他人的生物特征同样适用,并且其去身份识别的过程是可逆的。

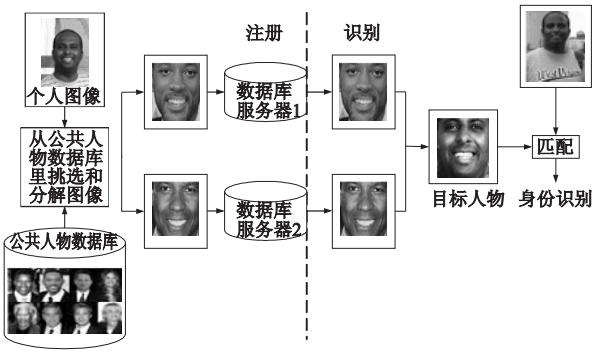

图2　脸部去身份识别方法框图

3.2　基于其他生物信息的去识别研究

有些去身份识别算法对于去除生物信息特征来说是通用的[36],例如上文提到的文献[35]所论述的方法对于去除指纹、虹膜、脸这三种生物信息特征都是有效的。一些加密算法对于以上三种生物信息是可以解决一定的去识别问题的。

针对说话人声音的安全保护工作需要完成以下两方面的内容:首先要确保说话人的声音所携带内容的安全,其次要对说话人的身份进行保护。也就是说,对于声音的去识别技术就是将原有的说话人的声音进行处理后,在保证不泄露说话人身份的同时完好地保留声音所表达的内容。文献[37]针对不同的声音研究了多种变换策略,通过声音变换达到去识别的效果,并且通过两种识别算法验证了该算法的有效性和鲁棒性。

影响去身份识别的生物因素中的人体轮廓和步态信息是需要进一步重点研究的方面。这是因为它们是影响去身份识别的生物信息因素中最难以去除的部分。由于这些生物特征与人的动作行为息息相关[38],而去身份识别过程要在去除这些特征的同时保证对目标进行行为识别的可靠性,所以对于它们的去识别研究就更加困难和复杂。也就是说在去身份识别的过程中需要去除可以识别人物身份的信息(包括人体轮廓和步态信息等)。例如在步态识别研究过程中提取到的特征向量,在去身份识别以后这些特征就无法通过步态识别进行身份认定了。目前关于这方面的研究还较为稀少。Chen 等人[39]提出了一种能够在医院视频中去除个人显著特征的隐私保护系统,并且通过一定的数据进行了验证,并且他们还提出了一种利用人体边缘运动轨迹信息来进行人的整体外形轮廓模糊化的去识别方法。而这种方法有一定的局限性,它在模糊化后的图像信息无法进行动作行为识别。Dufaux 等人[40]提出的方法是,首先在输入视频中使用背景差除法提取目标,然后打乱在感兴趣区域中被用于编码的运动 JPEG 压缩视频序列的系数,通过以上方法可以完成对原始图像的去身份识别。Park 等人[41]提出了一种图色覆盖的去识别算法。通过用基色相似的像素点对前景信息进行点图覆盖,并用图框进行运动目标跟踪。Chinomi 等人[42]也针对前景人物可完全被覆盖的视频提出了用背景颜色或者纯色填充目标边界框的方法。对于人体轮廓和步态信息去识别的最新研究是 2011 年 Agrawal 等人提出的方法,他们在文献[8]中提出了既能去除人的脸部和轮廓信息以及步态信息,又能对模糊化以后的图像进行运动行为识别的去身份识别方法,并用目前比较通用的几种身份识别算法进行了验证,结果表明模糊化算法可以使自动识别身份算法失效。图 3 显示了三段视频使用文献[8]中的去身份识别算法后的关键帧效果图,图中可以清楚地显示前景人物的动作行为依次为:打电话、挥手和散步,但是对于人物的身份已经无法辨别了。也就是说在去除了人脸、轮廓、步态这些生物信息的基础上,达到了仍然可以进行动作行为识别的效果。

图3　不同动作行为的去身份识别效果

4　存在的问题及挑战

综合以上对当前研究的论述和分析,对去身份识别研究存在的问题及挑战概括如下:

a)性能评估标准的统一化。目前,对去身份识别算法的验证,基本上都是各个学者根据自己的数据库和所挑选的识别算法进行验证。由于缺乏通用的数据库及其规模限制,当前对去身份识别算法的性能评估还没有形成统一的标准。纵观去身份识别算法研究现状,有些算法只是完成了去识别的效果并未进行评估,有些采用的数据库规模较小只包含几十个样本,有些通过人的肉眼来判定去身份识别的效果,这就使得无法对各种去身份识别算法的效果进行统一的准确的评价和比较。

b)数据存储。为了安全考虑,对于去识别后的数据信息往往都是需要进行存档的,以便日后调用。针对去身份识别的视频及图像数据的存储基本分为两类:一类是原始数据可以丢弃的,另一类是原始数据需要保存的。对于前者而言,去身份识别数据只需要实时被获得,而不需要被保存或者只需要挑选

有异常的个别数据进行保存。这种情况对于存储空间的要求较低,占用资源相对较少。对于后者来说又分为两种情况:一种是对去身份识别的数据和加密的去身份算法参数进行保存,通过算法参数可以对去身份识别的数据进行还原得到原始数据;另一种是对去身份识别的数据和高度加密的原始数据进行保存。这是由于去身份识别的数据是采用的高度随机算法进行处理,往往是无法对数据进行还原的,为了保护和保存原始数据,只能对其也进行加密处理。这种情况下对于存储空间的要求较高,占用资源相对较多。

c)算法复杂度计算。越靠近视频获取端进行图像保护处理,对数据而言最安全。如果对数据进行传输后在控制端进行处理的话,就还要考虑数据传输过程中的安全问题。也就是说去身份识别算法的完成最后要集成在照相机、监控摄像头等终端,这样可以最大程度地保护数据的私密性。由于视频获取终端越来越集成化和小型化,去身份识别算法在能够完成去识别效果的同时,其算法复杂度越低越好。

d)算法本身的难点。主要包括以下方面:

(a)对于去身份识别后数据的完整性要求。去身份识别后的数据信息,只是对前景的信息进行处理,对于背景以及前景的行为动作信息要进行完整的保留。越是良好的去身份识别算法对于背景以及前景的行为动作信息保留得越多。

(b)对于去身份识别算法的健壮性要求。为了起到对个人身份信息的保护作用,去身份识别算法实现以后使用任何的识别算法都无法从数据中识别出人的身份。对于识别算法中提取的特征,在去识别的过程中都是需要考虑的,并且生物信息中的脸、指纹、虹膜、外形轮廓、步态、声音等因素在去识别过程中所占有的权重是需要进一步考量的。对于在去识别过程中占有很高比重的因素应该被尽量多地得到重视。

(c)对于去身份识别算法参数选择的保密性要求。去身份识别算法变换过程的参数应该是完全保密的,否则对于个人信息的保护作用就失效了。鉴于这种情况,对于一些去识别变换过程中的参数是随机选取的,因此这个随机函数就显得尤为重要,并且是一个可以深入研究的方面。

5 结束语

去身份识别作为生物特征领域的一个最新研究方向,已经引起了广大科研工作者强烈的兴趣。通过研究人员不懈的努力,去身份识别技术已经展示了其强大的性能和巨大的潜能,并且正在日臻完善。本文从影响去身份识别的因素出发,结合当前研究的现状,综述了去身份识别的各种方法,并在此基础上阐述了去身份识别目前仍然存在的问题及挑战。

参考文献:

[1] ANGUELOV D, DULONG C, FILIP D, *et al*. Google street view: capturing the world at street level[J]. Computer,2010,43(6): 32-38.

[2] HELD C, KRUMM J, MARKEL P, *et al*. Intelligent video surveillance[J]. Computer,2012,45(3): 83-84.

[3] NEWTON E M. Biometrics and surveillance: identification, de-identification, and strategies for protection of personal data[D]. Pittsburgh, Pennsylvania: Carnegie Mellon University Carnegie Institute of Technology,2009.

[4] KOSHIMIZU T, TORIYAMA T, NOBORU B. Factors on the sense of privacy in video surveillance[C]//Proc of the 3rd ACM Workshop on Continuous Archival and Retrival of Personal Experences. 2006: 35-44.

[5] SENIOR A W, PANKANTI S, HAMPAPUR A, *et al*. Enabling video privacy through computer vision[J]. IEEE Security and Privacy, 2004,3(3):50-57.

[6] BOYLE M, EDWARDS C, GREENBERG S. The effects of filtered video on awareness and privacy[C]//Proc of ACM Confe-rence on Computer Supported Cooperative Work. 2000:1-10.

[7] WANT R, HOPPER A, FALCAO V, *et al*. The active badge location system[J]. ACM Trans on Information Systems,1992,10(1): 91-102.

[8] AGRAWAL P, NARAYANAN P J. Person de-identification in videos [J]. IEEE Trans on Circuits and Systems for Video Technology,2011,21(3):299-310.

[9] AGGARWAL C C, YU P S. Privacy-preserving data mining: models and algorithms[M]. New York: Springer Science + Business Media, 2008.

[10] SENIOR A W. Privacy enablement in a surveillance system[C]// Proc of IEEE International Conference on Image Processing. 2008: 1680-1683.

[11] YU X, CHINOMI K, KOSHIMIZU T, *et al*. Privacy protecting visual processing for secure video surveillance[C]//Proc of IEEE International Conference on Image Processing. 2008:1672-1675.

[12] REN X, BERG A C, MALIK J. Recovering human body configurations using pairwise constraints between parts[C]//Proc of the 10th IEEE International Conference on Computer Vision. 2005: 824-831.

[13] MORI G, MALIK J. Recovering 3-D human body configurations using shape contexts[J]. IEEE Trans on Pattern Analysis and Machine Intelligence,2006,28(7): 1052-1062.

[14] WICKRAMASURIYA J, ALHAZZAZI M, DATT M, *et al*. Privacy-protecting video surveillance[C]//Proc of SPIE Conference on Real-time Imaging. 2005: 64-75.

[15] BRASSIL J. Using mobile communications to assert privacy from video surveillance[C]//Proc of the 19th IEEE International Symposium on Parallel and Distributed. 2005.

[16] ZHANG W, CHEUNG S C S, CHEN M. Hiding privacy information in video surveillance system[C]//Proc of International Conference on Image Processing. 2005: 868-871.

[17] CHEUNG S C S, PARUCHURI J K, NGUYEN T P. Managing privacy data in pervasive camera networks[C]//Proc of International Conference on Image Processing. 2008:1676-1679.

[18] SWEENEY L, GROSS R. Mining images in publicly-available cameras for homeland security[C]//Proc of AAAI Spring Symposium on AI Technologies for Homeland Security. 2005: 161-163.

[19] SCHIFF J, MEINGAST M, MULLIGAN D K, *et al*. Respectful cameras: detecting visual markers in real-time to address privacy concerns[C]//Proc of IEEE/RSJ International Conference on Intelligent Robots and Systems. 2007: 971-978.

[20] WINKLER T, RINNER B. Trustcam: security and privacy-protection for an embedded smart camera based on trusted computing[C]//Proc of the 7th IEEE International Conference on Advanced Video and Signal Based Surveillance. 2010: 593-600.

[21] CHATTOPADHYAY A, BOULT T E. Privacycam: a privacy preser-

ving camera using UCLinux on the blackfin DSP[C]//Proc of the 3rd IEEE Workshop on Embedded Vision Systems. 2007.

[22] MRITYUNJAY M, NARAYANAN P J. The de-identification camera [C]//Proc of the 3rd National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics. 2011:192-196.

[23] AGARWALA A, DONTCHEVA M, AGRAWALA M, *et al*. Interactive digital photomontage[J]. ACM Trans on Graphics,2004,23(3): 294-302.

[24] BLANZ V, SCHERBAUM K, VETTER T, *et al*. Exchanging faces in images[J]. Computer Graphics Forum,2004,23(3): 669-676.

[25] NISHIYAMA M, TAKESHIMA H, SHOTTON J, *et al*. Facial deblur inference to improve recognition of blurred faces[C]//Proc of IEEE Conference on Computer Vision and Pattern Recognition. 2009: 1115-1122.

[26] NEWTON E, SWEENEY L, MALIN B. Preserving privacy by de-identifying facial images[J]. IEEE Trans on Knowledge and Data Engineering,2005,17(2): 232-243.

[27] GROSS R, AIROLDI E, MALIN B, *et al*. Integrating utility into face de-identification[C]//Proc of Workshop on Privacy Enhancing Technology. 2005: 227-242.

[28] GROSS R, SWEENEY L, De la TORRE F, *et al*. Semi-supervised learning of multi-factor models for face de-identification[C]//Proc of IEEE Conference on Computer Vision and Pattern Recognition. 2008: 1-8.

[29] GROSS R, SWEENEY L, De la TORRE F, *et al*. Model-based face de-identification[C]//Proc of Conference on Computer Vision and Pattern Recognition Workshop. 2006: 161-169.

[30] GROSS R, SWEENEY L. Towards real-world face de-identification [C]//Proc of IEEE International Conference on Biometrics: Theory Applications and Systems. 2007: 1-8.

[31] PHILLIPS P. Privacy operating characteristic for privacy protection in surveillance applications[C]//Proc of the 5th International Conference on Audio-and Video-based Biometric Person Authentication. 2005: 869-878.

[32] FROME A, CHEUNG G, ABDULKADER A, *et al*. Large-scale privacy protection in Google street view[C]//Proc of the 12th International Conference on Computer Vision. 2009: 2373-2380.

[33] SEO J S, HWANG S O, SUH Y H. A reversible face de-identification method based on robust hashing[C]//Proc of International Conference on Consumer Electronics. 2008: 1-2.

[34] BITOUK D, KUMAR N, DHILLON S, *et al*. Face swapping: automatically replacing faces in photographs[J]. ACM Trans on Graphics,2008,27(3): 1-8.

[35] ROSS A, OTHMAN A. Visual cryptography for biometric privacy [J]. IEEE Trans on Information Forensics and Security,2011,6(1): 70-80.

[36] NEUSTAEDTER C, GREENBERG S, BOYLE M. Blur filtration fails to preserve privacy for home-based video conferencing[J]. ACM Trans on Computer Human Interactions,2006,13(1): 1-36.

[37] JIN Qin, TOTH A R, SCHULTZ T, *et al*. Voice convergin: speaker de-identification by voice transformation[C]//Proc of IEEE International Conference on Acoustics Speech and Signal. 2009: 3909-3912.

[38] 贲晛烨,徐森,王科俊. 行人步态的特征表达及识别综述[J]. 模式识别与人工智能,2012,25(1):71-81.

[39] CHEN Da-tong, CHANG Yi, YAN Rong, *et al*. Tools for protecting the privacy of specific individuals in video[J]. EURASIP Journal on Applied Signal Processing,2007,2007(1): 107.

[40] DUFAUX F, EBRAHIMI T. Scrambling for privacy protection in video surveillance systems[J]. IEEE Trans on Circuits and Systems for Video Technology,2008,18(8): 1168-1174.

[41] PARK S, TRIVEDI M. A track-based human movement analysis and privacy protection system adaptive to environmental contexts[C]// Proc of IEEE Conference on Advanced Video and Signal Based Surveillance. 2005: 171-176.

[42] CHINOMI K, NITTA N, ITO Y, *et al*. Prisurv: privacy protected video surveillance system using adaptive visual abstraction[C]//Proc of International Multimedia Modeling Conference. 2008:144-154.

(上接第 333 页)

[12] ZOU Yi, CHAKRABARTY K. Fault-tolerant self-organization in sensor networks[C]//Proc of DCOSS. Heidelberg: Springer-Verlag, 2005:191-205.

[13] GABRIELLI A, MANCINI L V, SETIA S, *et al*. Securing topology maintenance protocols for sensor networks[J]. IEEE Trans on Dependable and Secure Computing,2011,8(3):450-465.

[14] 康一梅,李志军,胡江,等. 一种低能耗层次型无线传感器网络拓扑控制算法[J]. 自动化学报,2010,36(4): 543-549.

[15] 魏永红,李孝忠. 分簇及局部优化的无线传感器网络拓扑控制算法[J]. 天津科技大学学报,2010,25(2):68-71.

[16] QURESHI H K, RIZVI S, SALEEM M, *et al*. Poly: a reliable and energy efficient topology control protocol for wireless sensor networks [J]. Computer Communications,2011,34(10): 1235-1242.

[17] 沈中,常义林,崔灿,等. 一种建立可自维护且具有最小能量特性的无线网络的分布式拓扑控制算法[J]. 计算机学报,2007,30(4):569-578.

[18] YIN Rong-rong, LIU Bin, HAO Xiao-chen. An energy efficient topology maintenance scheme for wireless sensor networks[J]. Journal of Information and Computational Science, 2011, 8(13): 2815-2822.

[19] XU Ya, HEIDEMANN J, ESTRIN D. Adaptive energy-conserving routing for multihop Ad hoc networks, TR-2000-527[R]. [S. l.]: USC/ISI, 2000.

[20] BALA K M, DOJA M N. Swarm intelligence based topology maintenance protocol for wireless sensor networks[J]. IET Wireless Sensor Systems,2011,1(4):181-190.

[21] WENDI R H, ANANTHA C, HARI B. Energy-efficient communication protocol for wireless microsensor networks[C]//Proc of the Hawaii International Conference on System Science. 2000:223-232.

[22] ZHAO Nan-nan, WU Mu-qing, ZHANG Yu. A localized MESH-CDS structure and maintenance for wireless sensor networks[C]//Proc of the 6th International Conference on Wireless and Mobile Communications. [S. l.]: IEEE Computer Society,2010:262-267.

[23] SZCZYTOWSKI P, KHELIL A, SURI N. DKM: distributed *k*-connectivity maintenance in wireless sensor networks[C]//Proc of the 9th Annual Conference on Wireless On-demand Network Systems and Serrices. [S. l.]: IEEE Computer Society,2012:83-90.

[24] CHOU C A, SSU K F, JIAU H C, *et al*. A dead-end topology maintenance protocol geographic forwarding in wireless sensor networks [J]. IEEE Trans on Computers,2011,60(11):1610-1621.