文章编号:1001 - 9081(2010)03 - 0657 - 06

数字多媒体取证技术综述

胡永健,刘琲贝,贺前华
(华南理工大学 电子与信息学院,广州 510641)
(eeyjhu@scut.edu.cn)

摘　要:数字多媒体取证是信息安全一个刚刚兴起的研究领域,研究数字多媒体取证技术对确保多媒体数据的可靠性有着极其重要的意义。以数字图像取证为代表,从篡改检测、来源辨识、真实性鉴定、设备成分取证以及多媒体取证方法的可靠性等五个方面对现有数字多媒体取证技术进行综述,重点介绍了典型算法,并指出当前研究中存在的一些主要问题,给出本领域未来的研究方向。

关键词:数字多媒体取证;篡改检测;源设备辨识;设备成分取证;真实性鉴定;取证攻击
中图分类号: TP391　　**文献标志码**:A

Survey on techniques of digital multimedia forensics

HU Yong-jian, LIU Bei-bei, HE Qian-hua
(*School of Electronic and Information Engineering, South China University of Technology, Guangzhou Guangdong* 510641, *China*)

Abstract: Digital multimedia forensics is an emerging research field of information security. The research on digital multimedia forensics is important to ensure the credibility of digital multimedia data. Using digital image forensics as an example, the authors reviewed the current digital multimedia forensics techniques from the five aspects, including tamper detection, source device identification, authenticity verification, device component forensics, and the reliability of digital multimedia forensics. The authors focused on introducing typical algorithms, and meanwhile, pointed out the main problems in the current research and suggested the urgent topics for the future research.

Key words: digital multimedia forensics; tamper detection; source device identification; device component forensics; authentication verification; forensics attack

0　引言

功能强大的多媒体编辑软件使修改数字图像和音/视频数据变得简单和有趣。尽管普通人对数字图像等多媒体的修改只是为了增强表现效果,但也不乏有人出于各种目的,无意或者故意,甚至恶意地传播经过精心伪造的数字图像和音/视频数据。篡改和伪造的数字图像和音/视频一旦被大量地用于正式媒体、科学发现、保险和法庭证物等,无疑会对政治、军事和社会的各方面产生严重的影响[1]。因此,需要一种客观、公正、能够澄清事实真相的验证技术,数字多媒体取证(digital multimedia forensics)正是为这一目的而提出的。数字多媒体取证主要按以下两个原理工作:1)通过对多媒体数据特征进行分析来判断多媒体内容的完整性、原始性和真实性;2)通过对残留在多媒体数据内部的设备印迹以及数字信号后处理噪声进行分析来追溯多媒体数据的来源。

根据应用场合不同,目前国内外数字多媒体取证研究主要围绕以下五个方面展开:1)多媒体数据的篡改检测;2)多媒体数据的来源辨识;3)多媒体设备的成分取证;4)多媒体数据的真实性鉴定;5)多媒体取证的可靠性。在媒体类型方面,数字图像仍是目前的主要研究对象。本文以数字图像为代表,兼顾数字音/视频媒体类型,从以上几个方面对现有的数字多媒体取证研究成果进行阐述,并指出当前研究中存在的一些主要问题,给出未来的研究发展方向。

1　多媒体数据的篡改检测

篡改检测主要是为了解决数字多媒体数据的完整性和原始性鉴定问题。传统的数字水印技术可以作为篡改检测的一种手段,但在现实世界中,绝大多数多媒体数据没有嵌入水印信息,因此,依赖水印的方法不太现实。另一方面,任何形式的篡改操作都会不可避免地引起多媒体数据内部特征尤其是统计特征的变化,由此可以借助不需要外部嵌入信息的数字取证方法来实现篡改检测。以下分别介绍数字图像、音频和视频的篡改检测方法。

1.1　数字图像的篡改检测方法

数字图像的篡改检测方法大致可归纳为五类[2]。

1)基于像素的检测方法。通过检测像素级别上的统计异常信息可判断图像是否经过篡改。文献[3 - 4]针对最为常见的复制—粘贴(copy-paste)篡改类型提出搜索图像中有无完全相同的区域,其中文献[3]是通过比较离散余弦变换块的系数,而文献[4]是通过比较图像块的主元分量。这类方法的原理很简单,关键是如何提高块的搜索效率以及抵抗由加性噪声和有损压缩而引起的图像像素的轻微变化。文献[5 - 7]则提出依据重采样所导致的特殊周期性进行篡改检测。复制—粘贴篡改往往伴随有缩放、旋转和拉伸等操作,而缩放、旋转和拉伸操作可以看成是图像信号向上和向下采样的组合,即发生多重采样,这会在图像信号中留下重采样痕

收稿日期:2009 - 09 - 21;**修回日期**:2009 - 11 - 16。

作者简介:胡永健(1962 -),男,湖北武汉人,教授,博士,主要研究方向:数字多媒体取证、信息隐藏、图像处理、模式识别;　刘琲贝(1980 -),女,广东广州人,博士,主要研究方向:数字多媒体取证、图像处理、模式识别;　贺前华(1965 -),男,湖南邵东人,教授,博士生导师,博士,主要研究方向:语音信号处理、优化算法、信号处理算法的嵌入式实现。

www.joca.cn 计算机应用 Journal of Computer Applications

迹,使图像中像素与其周围像素之间产生周期性的相关性。文献[8]针对拼—接合成篡改操作提出利用像素的高阶统计特性进行检测,特征向量由图像质量的评价测度和统计矩特征量联合构成。文献[9]提出了检测图像篡改更通用的方法,它首先使用三类取证特征,包括图像质量特征、二值相似度测度以及高阶小波系数统计特征,其中图像质量特征又包括基于像素差的测度、基于相关性的测度、基于边缘的测度、基于人类视觉特征的测度和基于频谱距离的测度,然后分为透视、半盲和全盲三种模式来讨论篡改问题。在透视模式下,篡改的类型和强度都已知,可比较各种方法对于篡改操作的敏感度;在半盲模式下,已知篡改的类型,可通过比较上述三类测度的改变来确定篡改强度;在全盲模式下,篡改的类型未知,通过设计不同的盲分类器来实现对不同类型篡改的检测。

2)基于压缩格式的检测方法。取证的首要准则是保护证据,从这层意义上说,有损图像压缩方案(如JPEG)可能是取证分析的最大障碍。然而,具有讽刺意义的是有损压缩所具有的独特特性可被用于取证分析[10]。JPEG是使用最普遍的图像压缩格式,检查JPEG图像篡改的主要途径有两个:双重JPEG压缩和JPEG的块效应。通常,原始图像和篡改后的图像都用JPEG格式保存,尽管双重JPEG压缩不一定表示图像被篡改,但这类图像有被篡改的嫌疑。文献[11]分析了离散余弦变换(Discrete Cosine Transform, DCT)系数的直方图在单次和两次压缩下的不同,给出了估计第一次压缩时所使用的量化系数的两种方法:第一种方法利用不同量化因子进行穷举试探;第二种方法利用神经网络分类器进行分类。前一种方法计算量大,而后一种方法计算量相对较小。文献[10]指出在一定条件下双重压缩DCT系数的直方图上存在周期性的噪声,利用DCT系数直方图的傅里叶变换可以估计出第一次压缩所使用的质量因子。文献[12]则给出检测JPEG二次压缩的较新方法,它用JPEG图像中当前像素与其四邻的差值构成一个新的二维矩阵,并用一步Markov随机过程来描述这个差值矩阵。由于二次JPEG压缩减弱了上述差值矩阵中元素之间的相关性,所以可通过分析差值矩阵中元素相关值的分布来确定是否发生二次JPEG压缩。除了利用双重JPEG压缩的特征外,JPEG的块效应是否遭到破坏也被广泛用于篡改检测。文献[13]引入一个块效应特征矩阵来反映未经剪切或再压缩图像的对称性,并指出这个对称性在遭到剪切或再压缩后会被破坏。文献[14]则利用DCT系数直方图的能谱在图像修改前后的二阶差分的极小值来估计量化系数,然后通过计算并比较各块噪声测度确定是否发生篡改以及发生篡改的位置。文献[15-16]提出依据图像各分块之间的量化系数是否一致和分块位置是否错位来检测图像的完整性。

3)基于成像设备特性的检测方法。受工作原理和物理特性的影响,数码相机的镜头、成像传感器和数字信号后处理会在成像过程中留下特有的设备痕迹和噪声,通过检查设备痕迹和噪声的一致性可判断是否发生篡改。例如,一幅自然图像内的色彩偏差应该是一致的,而篡改操作会破坏这种一致性。文献[17-18]根据色彩偏差的一致性判断图像是否发生篡改。又如,由于目前大部分数码相机只有一片CCD或CMOS成像传感器,所获得的彩色图像都是借助颜色滤波器阵列(Color Filter Array, CFA)的插值运算(也称去马赛克运算)得到,而不同数码相机采用的插值方法不同,常见的插值种类包括双线性插值、双三次插值、基于色调缓慢变换的插值、根据梯度判断边缘走向从而沿边缘进行的插值以及基于自适应原则的插值,所有这些插值运算都会在图像的各个色彩通道内、像素间引入特殊的周期性的统计相关性。文献[19]通过检测插值像素的周期相关性是否被破坏判断图像是否经过篡改。文献[20]对文献[19]所采用的检测周期性的最大似然估计迭代算法——EM(Expectation/Maximization)算法进行了改进,提高了计算效率。文献[21-22]通过检查图像内相机响应函数(Camera Response Function, CRF)的一致性来判别图像的篡改历史。文献[23]从图像去噪、小波系数分析和邻域预测等三个方面提取了60个统计噪声特征,利用支持向量机对统计噪声特征分类来确定图像是否发生篡改。文献[24]将相机的成像环节中噪声模型参数的一致性作为图像篡改的检测依据。

4)基于物理原理的检测方法。光照条件尤其适合于检测拼接—合成类型的篡改图像。通过检测物理对象、光线和相机在三维空间中两两交互作用之间的异常可以判断图像是否发生篡改。图像篡改可归结为对图像内容的增、删、改操作,一般是将一幅图像中的对象或背景与另一幅图像的背景或对象重新组合形成伪造图像,或是删除图像中的某一对象或背景来隐藏重要的目标。这些操作通常会破坏自然图像的光照一致性,而篡改操作很难把光照效果和定向的光源相匹配,因此,可根据图像中场景的光照不一致性鉴别图像的篡改。基于光学原理检测方法的关键是建立物理对象、光线和相机之间的光照模型。文献[25-26]分别给出了单光源下二维和三维的光照模型。由于自然场景的光源通常不止一个,文献[27]对多光源复杂环境下的成像进行了讨论,并给出了一个复杂光源环境的低参数近似模型。

5)基于对象几何关系的检测方法。照相机中心在图像平面上的投影点称为“主点”。在所拍摄的图像中,主点位于图像中心附近。当图像中的人或物平移时,主点也成比例地平移。文献[28]通过检验从图像的不同局部所估计出的主点位置是否一致来判断图像内容是否经过了改动。

归纳起来说,图像篡改检测方法中前三类的理论基础是数字图像处理、信号处理和模式识别,而后两类的理论基础则是计算机视觉和光学物理。

1.2 数字音频的篡改检测方法

针对模拟音频篡改检测的研究40年前就有了,而针对数字音频篡改检测的研究则刚开始[29],公开的研究成果相当少。文献[30]在对数字音频格式、篡改软件、音频分析的校验元组进行分析后,指出可分别在音频波形统计特征、音频附带背景噪声和音频格式附加信息等三方面进行篡改检测。“天然”音频信号在频域上具有很弱的高阶相关性,而大多数篡改操作都会引入一定的非线性,从而导致信号高阶相关性增强,使原来在真实人声频域上很弱的统计相关性变为较为显著的高阶统计相关性。文献[31]据此检测音频文件是否经过篡改。另一方面,文献[32]受图像篡改检测方法的启发,利用重采样信号的周期性检查音频中所发生的篡改。不过音频信号的插值检测和图像有所不同:第一,音频在短时内有静音存在;第二,即使没有插值过的音频的局部也可能呈现很强的线性相关。这两点使得EM迭代算法无法收敛到理想的结果。为此,文献[32]提出引入音频幅度直方图,排除短时静音和增加样本点数,以使图像的重采样检测算法能有效

www.joca.cn 计算机应用

地用于音频信号的篡改检测。文献[31]指出还可利用音频文件的格式信息进行篡改检测。音频文件格式种类繁多,不同格式的数字音频通常都包含一些必要的附加信息,包括日期、作者、编码格式等。对数字音频材料的篡改很有可能会改变这些附加信息,从而留下篡改痕迹。

1.3　数字视频的篡改检测方法

与数字图像相比,数字视频的获取设备以及编辑软件的普及度较低,相应的,针对数字视频的取证技术也起步较晚,目前公开的主要成果有文献[[33-35]。文献[33]是图像双重压缩篡改检测方法在视频中的延伸。在 MPEG 文件中,I、P、B 帧的编码方式不同,I 帧只依赖于自身信息进行 JPEG 压缩编码,P 帧依赖于前面的 I 帧或 P 帧的运动估计和运动补偿编码,而 B 帧则利用过去、将来或者同时利用过去和将来的 I 帧或 P 帧作运动估计,再按类似于 P 帧的方式进行编码。当受到篡改时,可能发生帧丢失。通过计算 MPEG 视频流中每个 P 帧的运动误差以及全部帧的平均运动误差,观察运动误差中周期性的噪声,可以确定是否发生篡改。文献[34]讨论了两种情形下的篡改检测:第一种是针对消除隔行扫描后的视频;第二种是针对隔行扫描的视频。对于第一种情况,由于消除隔行扫描的两种基本算法是场合并和场扩展,如果将这两种算法看成是一种周期性的插值模式,则可利用 EM 算法来检测插值的周期性。当周期性遭到破坏时,可认为视频遭到篡改。对于第二种情况,通过检测一帧内两个场的运动或相邻帧中场的运动情况,可判断有没有发生篡改。在没有篡改过的视频中,运动是相等的;而在篡改过的视频中,两者不同。文献[35]利用模式噪声对数字视频进行篡改取证。由于成像传感器以及摄像机内部电路存在非理想性,在成像过程中必然会产生设备噪声,并被添加到每一帧视频中,而来自同一台摄像机拍摄的视频所包含的噪声存在着相关性。借用同种图像篡改检测的思想,检测前可先从参考视频中计算出摄像机的参考模式噪声,再从待检测视频帧中计算出噪声图像,将噪声图像与参考模式噪声作相关性比较,就可确定是否发生篡改,并可标定出篡改的位置。

2　多媒体数据的来源辨识

数字多媒体源设备辨识依赖于这样的假设:同一设备所获取的所有多媒体数据均带有该设备的内在特征,这些特征只与成像/录音管道以及该设备独有的硬件元器件有关,与多媒体数据所表达的内容无关。源设备辨识包含几个不同的层面:设备类型、设备品牌、设备型号以及设备个体,其中设备类型可以是照相机、扫描仪、摄像机、手机和录音机等,设备个体指某一台特定设备。

现有的源设备辨识研究成果主要集中在数字图像,还未见到有关音频和视频的源设备辨识工作。不同品牌的数码相机通常使用不同的镜头和成像传感器,并且采用不同的数字信号后处理运算,包括去马赛克、伽马矫正、色彩矫正、白平衡、压缩以及存储等。因此,即使拍摄同一对象,所生成的数字图像不仅在风格上有所不同,在图像质量上也存在细微差异。提取并分析这些差异特征,可实现对图像生成设备的源辨识。图像源辨识方法主要有三类:第一类提取色彩、图像质量、小波系数、镜头径向失真等统计特征,然后采用模式分类器对图像来源进行分类;第二类提取由成像设备固有缺陷导致的异常像素点和模式噪声等信息,通过比较相关性来确定源设备;第三类仅针对数码相机,将数码相机的 CFA 插值所导致的图像像素周期性统计特征作为辨识依据。下面分类进行介绍。

第一类方法的典型代表有文献[36,38]。文献[36]利用了 34 个图像特征,包括彩色图像 R(红)、G(绿)、B(蓝)各个通道上的像素均值,彩色通道 RB、BG、GR 之间的相关性,各通道上像素相邻分布(统计与各个像素的像素值相差在 ±1 之间的像素个数)的质心,三个彩色通道上图像两两之间的能量比,每个通道上图像三级小波变换后各个子带图像小波系数的均值。除了这些与彩色有关的特征外,还利用了不同相机产生不同质量的图像的特点。客观的图像质量测度可分为三类:基于像素值差异的测度(如均方差、差的绝对值的均值等);基于相关性的测度(归一化互相关等),基于频谱距离的测度(频谱的相角和幅值差等)。这些特征构成特征向量,作为支持向量机[37]的输入,进行源设备分类。文献[38]利用了相机镜头特有的径向失真。为了降低生产成本,大部分相机安装了球面镜头。不同型号的相机所安装的镜头不同,其径向失真也不同,因此球面镜头本身的径向失真可以作为设备指纹使用。径向失真的数学表达可由无穷级数描述。文献[38]以一幅图像的中心为原点,取级数的一阶和二阶系数 k_1 和 k_2 描述径向失真的程度。k_1 和 k_2 可单独组成特征向量作为支持向量机的输入,也可和文献[36]中的34 个图像特征联合组成特征向量。利用径向失真作为特征进行分类的主要障碍是径向失真具有随焦距变动而改变的特点,这导致同一镜头的 k_1 和 k_2 不恒定。

第二类方法的思想最早由 Fridrich 等人[39]提出。由于材料的缺陷、工艺的不完善以及半导体的电子噪声,任何成像传感器都有其固有的模式噪声。传感器的模式噪声主要由两部分构成:暗电流所引起的固定模式噪声(Fixed Pattern Noise, FPN)和光敏材料的光子响应非均匀性(Photo-Response Nonuniformity, PRNU)所引起的模式噪声。FPN 是加性噪声,中高档相机通过减去一个暗帧可以消除 FPN,所以不宜作为设备水印。但 PRNU 模式噪声(下文直接称为模式噪声)主要由半导体晶片的非均匀性和不完美性产生,一般不易消除,故可当做内部水印使用。模式噪声一个重要的性质是其高频分量与所拍摄的场景无关,并在相机的生命期中相对稳定。据此,若将模式噪声看成一个扩频水印,就可借助水印处理中基于相关性的检测手段来作出判断。文献[39]获得模式噪声的方法很简单,直接将多幅原始图像减去其低通滤波图像所得到的差值图像进行叠加再求平均,但这种方式所提取的模式噪声易受其他噪声的干扰,包括场景(或称背景)噪声、CFA 插值噪声和 JPEG 压缩噪声等。新的算法在检测前先对模式噪声作些预处理,以便去除不相干的噪声。例如,Alles 等人[40]提出消除 DCT 块效应,而 Fridrich 等人[41]则将原始图像减去其低通滤波图像所得到的图像认为是残差图像,然后根据统计信号估计理论,利用最大似然估计器从中估计出较精确的模式噪声。不过残差图像中场景噪声、CFA 插值噪声、JPEG 压缩量化噪声以及其他各类噪声的综合影响破坏了利用最大似然估计器所要求的高斯白噪声的假设,导致估计和检测不得不在近似满足高斯白噪声假设的各个分块进行,这使得整个算法的计算量较大。Goljan 等人[42-43]还将第二类方法应用到更复杂的场合,分别对剪切和拉伸后的图像以及从扫描仪所获取的图像进行了来源辨识。除了用于源设备

www.computerapplications.com.cn 计算机应用

辨识,Goljan等人[42-43]的第二类方法也可进一步推广到图像篡改检测,如文献[44-45],其工作原理是:若在同一图像中检测到不同成像设备所获取的图像局部,则可确定该图像内容遭到篡改。

第三类方法较特殊,它利用了大多数相机必须使用颜色滤波器这个事实。由于装有单片CCD或CMOS的相机只能通过颜色插值才能获得彩色图像,而不同厂家甚至不同型号的相机使用不同的插值算法,因此,只要能从测试图像中估计出插值周期,就可推算出所采用的插值算法,从而追溯出源相机。文献[46]首先提出这个思想。由于插值点的像素值是由邻域像素的值加权求和而来,文献[46]借助EM算法估计插值系数(即加权系数),并输出一个反映当前像素与其相邻像素相似性的二维概率图,然后在此基础上构造相机品牌的分类器。文献[47]进一步分析了常用的6种插值算法,并利用主元分析和神经网络估计插值系数。

归纳起来说,第一类方法利用了图像的统计特征,第二类方法利用了成像设备的机器指纹,而第三类方法利用了成像管道的特性。手机、扫描仪和打印机设备源辨识的方法主要借用了第一、二类相机源辨识的思想[48-51]。

3 多媒体设备的成分取证

成分取证的主要目标是辨别多媒体设备中各个组成元器件所使用的算法及其参数,其基本方法是寻找设备中各个处理模块在数字多媒体数据中遗留的痕迹,并据此估计出各模块的参数。成分取证具有广泛的实际应用前景,不但可用作多媒体数据的篡改鉴定,还可用于辨识多媒体数据的来源.例如,指出不同照相机之间在内部结构、零部件以及软件算法上的相似性,用于知识产权侵权案件的举证。

根据前提条件不同,成分取证有三种类型:侵入式取证(可获取设备并对其进行拆解)、半侵入式取证(可获取设备,但不可对其进行拆解)和非侵入式取证(无法获取设备,仅有设备产生的数据样本)。目前,成分取证主要集中在比较照相机响应函数、颜色滤波器阵列、颜色插值算法的参数以及插值后的信号处理运算上[52-53]。文献[52]给出了非侵入式取证的一般框架,并通过从数字图像中估计CFA的形式以及颜色插值算法的参数确定相机的生产厂家。文献[53]从模式分类理论的角度回答了哪些运算可分、哪些运算不可分,成分取证的限制是什么以及三种成分取证类型之间的关系。

成分取证可看成是多媒体源设备辨识的一种特殊情况,它更关注设备的内部结构,而非将设备看成一个整体。从技术层面上讲,多媒体源设备辨识的不少方法都可推广到成分取证。

4 多媒体数据的真实性鉴定

当今先进的计算机技术可生成以假乱真的图像、音频和视频,因此,在使用数字多媒体数据时,必须解决的一个问题就是真实性鉴定。由于计算机生成图像的技术最为成熟,计算机生成的图像也最为常见,因此,识别一幅图像是自然图像还是计算机生成的图像是目前真实性鉴定的研究重点。

当前普遍采用的技术路线是分别研究自然成像设备的成像原理以及计算机图形学中的真实感绘制技术,然后从两者的相似性和相异性中寻找辨别依据。对于低仿真度的计算机生成卡通图像,可以根据平均色彩饱和度、高亮像素比、色彩直方图、边缘检测、压缩比和粒度等图像特征组成特征向量,然后利用模式分类器进行分类识别,典型工作有文献[54]。对于高仿真度的计算机生成图像,文献[55]提出一个基于图像小波分解的统计模型用于描述自然图像,再从小波系数的线性预测和预测误差着手,构造了一个216维的特征向量作为支持向量机的输入。文献[56]提出一个基于几何学的图像描述方案,揭示自然图像和计算机生成图像在图像生成过程中的不同,它所使用的192个特征分别来自于局部斑纹统计量、线性高斯刻度空间、分形几何学和差分几何学。文献[57]改进了文献[55]的方法,在基于图像小波分解的统计模型上定义了不同的图像特征,得到比文献[55]更好的结果。文献[58]除了利用文献[55]中均值、方差、偏斜度和峰度这几个特征外,还增加了梯度能量特征,并采用另一种流行的分类算法AdaBoost,获得了更好的效果。不同于前面单纯从图像提取特征的方法,文献[59]利用了成像设备的物理特性,从去马赛克痕迹和色差出发,讨论自然图像和计算机生成图像之间的区别。具体来说,它利用4个基于去马赛克的特征和1个基于色差的特征,从灰度图像构造了一个72维的特征向量。文献[60]讨论了一个更为特殊的问题——计算机生成图像的"翻拍"辨识问题。翻拍图像的反射分量含有特殊的高频空间变化,它与打印表面的内部结构有关。通过比较原始图像反射分量的分布和翻拍图像反射分量的分布,可区分这两类图像。

利用自然图像的特征和成像管道的设备印迹是区分自然图像和计算机生成图像的关键,这个思想同样可以推广到音频和视频的真实性鉴定。

5 多媒体取证的可靠性

目前对数字图像取证可靠性进行研究的文章数量很少,正如文献[61]指出,本领域现有的大部分算法缺乏对鲁棒性进行严格的讨论,而狡猾的造假者对可能出现的取证技术早有防范。一般而言,针对数字多媒体取证技术的攻击有三类:对图像恶意处理或篡改后进行伪装;对图像的真实来源标识进行抑制;对图像的来源进行造假。为了证明攻击的有效性,该文进一步给出了两个实例,分别对目前流行的重采样检测方法[6]和基于模式噪声的检测方法[44]给出了攻击算法。最后该文给出了一个很有启发意义的图像取证策略,建议在取证之前先对图像进行篡改检测。尽管该文讨论的对象是数字图像,但所提出的攻击类型和取证策略可以直接推广到数字音频和视频。

据作者查找文献的情况来看,目前对多媒体取证可靠性的研究极为匮乏,除少量对数字图像取证技术可靠性进行初步研究的工作外,尚未发现有关音频和视频取证技术可靠性的研究。

6 结语

本文从五个方面对国内外数字多媒体取证技术的现状进行了综述。可以看到,尽管前四个方面的技术是针对不同应用场合提出的,但不少设计思想可以互相借用。从总体上看,现有数字多媒体取证方法还存在不少理论和技术层面的问题,解决这些问题对学科的发展至关重要,因此,寻找这些问题的解法必将是未来的重要研究内容。

第一,目前关于数字多媒体取证还没有形成清晰完整的

www.joca.cn 计算机应用

理论体系,大多数方法属于经验性的探索,尚有大量理论问题没有得到解决。例如,现有的取证技术主要依赖于比较设备特征信息,但学术界对什么样的特征信息可以用于取证却没有统一的认识。又如,尽管设备印迹可以看成是一种内部水印,但这种特殊水印在各个设备中的容量有多大,需要达到怎样的强度才能被检测以及以何种方式检测最佳等关键问题在目前的文献中缺乏讨论。

第二,现有的各类方法在技术实现上还面临较大困难,其中较为突出的一个问题是由于数字多媒体数据来源的多样性和内容的复杂性,导致目前基于数据自身统计特征的取证算法结果往往强烈依赖于训练样本的选择。同时,多数篡改检测算法针对性过强,适应性较弱,往往只针对某种特定的篡改类型,无法应对多种篡改联合伪造。

第三,目前的研究较多侧重于数字图像,然而,随着数字摄录设备的普及、存储成本的降低以及编辑软件的日益强大,音频和视频也逐渐成为人们保存多媒体数据的手段。因此,针对数字音频和视频的取证研究需要加强。

最后值得指出的是,数字多媒体取证技术本质上属于信息安全领域,而任何与安全有关的问题都必须讨论理论上和技术上可能存在的漏洞。现有文献极少对数字取证方法的攻击与反攻击问题进行讨论,这方面的研究亟须加强。

参考文献:

[1] 周林娜,王东明. 数字图像取证技术[M]. 北京:北京邮电大学出版社,2008.

[2] FARID H. Image forgery detection [J]. IEEE Signal Processing Magazine, 2009, 26(2): 16 – 25.

[3] FRIDRICH J, SOUKAL D, LUKAS J. Detection of copy move forgery in digital images [EB/OL]. [2009 – 06 – 15]. http://www.ws.binghamton.edu/fridrich/Research/copymove.pdf.

[4] POPESCU A, FARID H. Exposing digital forgeries by detecting duplicated image regions, TR2004-515 [R]. Hanover, NH: Dartmouth College, Department of Computer Science, 2004.

[5] MAHDIAN B, SAIC S. Blind authentication using periodic properties of interpolation [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(3): 529 – 538.

[6] POPESCU A C, FARID H. Exposing digital forgeries by detecting traces of resampling [J]. IEEE Transactions on Signal Processing, 2005, 53(2): 758 – 767.

[7] PRASAD S, RAMAKRISHNAN K. On resampling detection and its application to detect image tampering [C]// Proceedings of IEEE International Conference on Multimedia and Exposition. Toronto, Canada: IEEE Computer Society, 2006: 1325 – 1328.

[8] 张震,康吉全,平西建,等. 用统计特征量实现的图像拼接盲检测[J]. 计算机应用,2008,28(12):3108 – 3111.

[9] BAYRAM S, AVCIBAS I, SANKUR B, *et al*. Image manipulation detection [J]. Journal of Electronic Imaging, 2006, 15(4): 1 – 17.

[10] POPESCU A C, FARID H. Statistical tools for digital forensics [C]// Proceedings of International Workshop on Information Hiding. Toronto, Canada: IEEE Signal Processing Society, 2004: 128 – 147.

[11] LUKAS J, FRIDRICH J. Estimation of primary quantization matrix in double compressed JPEG images [EB/OL]. [2009 – 05 – 20]. http://www.ws.binghamton.edu/fridrich/Research/Doublecompression.pdf.

[12] CHEN C, SHI Y Q, WEI S. A machine learning based scheme for double JPEG compression detection [C]// Proceedings of 19th International Conference on Pattern Recognition. Tampa, Florida, USA: IEEE Computer Society, 2008: 1 – 4.

[13] LUO W, QU Z, HUANG J, *et al*. A novel method for detecting cropped and recompressed image block [C]// Proceedings of 2007 IEEE International Conference on Acoustics, Speech and Signal Processing. Honolulu, HI: IEEE Signal Processing Society, 2007: 217 – 220.

[14] YE S, SUN Q, CHANG E C. Detecting digital image forgeries by measuring inconsistencies of blocking artifacts [C]// Proceedings of 2007 IEEE International Conference on Multimedia and Expo. Washington, DC: IEEE Computer Society, 2007: 12 – 15.

[15] FARID H. Exposing digital forgeries from JPEG ghosts [J]. IEEE Transactions on Information Forensics and Security, 2009, 4(1): 154 – 160.

[16] 李晟,张新鹏. 利用 JPEG 压缩特性的合成图像检测[J]. 应用科学学报,2008,26(3):281 – 287.

[17] JOHNSON M, FARID H. Exposing digital forgeries through chromatic aberration [C]// Proceedings of ACM Multimedia and Security Workshop. Geneva, Switzerland: [s.n.], 2006: 48 – 55.

[18] 王波,孙璐璐,孔祥维,等. 图像伪造中模糊操作的异常色调率取证技术[J]. 电子学报,2006,34(12):2451 – 2454.

[19] POPESCU A, FARID H. Exposing digital forgeries in color filter array interpolated images [J]. IEEE Transactions on Signal Processing, 2005, 53(12): 3948 – 3959.

[20] 张雯,李学明. 改进的基于颜色滤波阵列特性的篡改检测[J]. 计算机工程与应用,2009,45(6):176 – 179.

[21] HSU Y-F, CHANG S-F. Image splicing detection using camera response function consistency and automatic segmentation [C]// Proceedings of 2007 IEEE International Conference on Multimedia and Expo. Beijing: IEEE Computer Society, 2007: 28 – 31.

[22] LIN Z, WANG R, TANG X, *et al*. Detecting doctored images using camera response normality and consistency [C]// Proceedings of 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Washington, DC: IEEE Computer Society, 2005: 1087 – 1092.

[23] GOU H, SWAMINATHAN A, WU M. Noise features for image tampering detection and steganalysis [C]// Proceedings of 2007 IEEE International Conference on Image Processing, San Antonio, TX: IEEE Signal Processing Society, 2007: 97 – 100.

[24] SWAMINATHAN A, WU M, LIU K J R. Digital image forensics via intrinsic fingerprints [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 101 – 117.

[25] JOHNSON M, FARID H. Exposing digital forgeries by detecting inconsistencies in lighting [C]// Proceedings of ACM Multimedia and Security Workshop. New York: ACM Press, 2005: 1 – 10.

[26] JOHNSON M, FARID H. Exposing digital forgeries through specular highlights on the eye [C]// Proceedings of the 9th International Workshop on Information Hiding. Saint Malo, France: IEEE Signal Processing Society, 2007: 311 – 325.

[27] JOHNSON M, FARID H. Exposing digital forgeries in complex lighting environments [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 450 – 461.

[28] JOHNSON M, FARID H. Detecting photographic composite of people [C]// IWDW 2007: Proceedings of the 6th International Workshop on Digital Watermarking. Berlin: Springer-Verlag, 2007: 19 – 33.

www.computerapplications.com.cn 计算机应用

[29] MAHER R C. Audio forensic examination [J]. IEEE Signal Processing Magazine, 2009, 26(2): 84 - 94.

[30] 高阳. 数字音频材料的真实性检测[D]. 上海: 上海交通大学, 2008.

[31] 高阳, 黄征, 徐彻, 等. 基于高阶频谱分析的音频篡改鉴定[J]. 信息安全与通信保密, 2008(2): 94 - 96.

[32] 姚秋明, 柴佩琪, 宣国荣, 等. 基于期望最大化算法的音频取证中的篡改检测[J]. 计算机应用, 2006, 26(11): 2598 - 2601.

[33] WANG W, FARID H. Exposing digital forgeries in video by detecting double MPEG compression [C]// Proceedings of the 8th Workshop on Multimedia and Security. New York: ACM Press, 2006: 37 - 47.

[34] WANG W, FARID H. Exposing digital forgeries in interlaced and deinterlaced video [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 438 - 449.

[35] 王俊文, 刘光杰, 张湛, 等. 基于模式噪声的数字视频篡改取证[J]. 东南大学学报: 自然科学版, 2008, 38(A02): 13 - 17.

[36] KHARRAZI M, SENCAR H T, MEMON N. Blind source camera identification [C]// Proceedings of 2004 International Conference on Image Processing. Washington, DC: IEEE Signal Processing Society, 2004: 709 - 712.

[37] CHANG C C, LIN C J. LIBSVM: A library for support vector machines [EB/OL]. [2009 - 06 - 05]. http://www.csie.ntu.edu.tw/~cjlin/libsvm/.

[38] CHOI K, LAM E, WONG K. Automatic source camera identification using the intrinsic lens radial distortion [J]. Optics Express, 2006, 14(24): 11551 - 11565.

[39] LUKAS J, FRIDRICH J, GOLJAN M. Digital camera identification from sensor pattern noise [J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 205 - 214.

[40] ALLES E J, GERADTS Z J M H, VEENMAN C J. Source camera identification for low resolution heavily compressed images [C]// Proceedings of 2008 IEEE International Conference on Computational Sciences and its Applications. Washington, DC: IEEE Computer Society, 2008: 557 - 567.

[41] CHEN M, FRIDRICH J, GOLJAN M, *et al.* Determining image origin and integrity using sensor noise [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 74 - 90.

[42] GOLJAN M, FRIDRICH J. Camera identification from cropped and scaled images [C]// Proceedings of SPIE, Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents X. San Jose, CA: SPIE, 2008: OE-1 - OE-13.

[43] GOLJAN M, FRIDRICH J, LUKAS J. Camera identification from printed images [C]// Proceedings of SPIE, Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents X. San Jose, CA: SPIE, 2008: 68190I. 1 - 68190I. 12.

[44] FRIDRICH J, LUKAS J, GOLJAN M. Detecting digital image forgeries using sensor pattern noise [EB/OL]. [2009 - 06 - 02]. http://adsabs.harvard.edu/abs/2006SPIE.6072..362L.

[45] 崔夏荣, 苏光大. 基于噪音相关性的数字图像区域作伪检测[J]. 光子学报, 2008, 37(10): 2108 - 2113.

[46] BAYRAM S, SENCAR H, MEMON N. Source camera identification based on CFA interpolation [C]// Proceedings of IEEE International Conference on Image Processing. Washington, DC: IEEE Signal Processing Society, 2005: 69 - 72.

[47] LONG Y, HUANG Y. Image based source camera identification using demosaicking [C]// Proceedings of the 8th Workshop on Multimedia Signal Processing. Washington, DC: IEEE Computer Society, 2006: 419 - 424.

[48] GOU H, SWAMINATHAN A, WU M. Robust scanner identification based on noise features [C]// Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX. San Jose, CA: SPIE, 2007: 65050S. 1 - 65050S. 11.

[49] KHANNA N, DELP E. Scanner identification using feature-based processing and analysis [J]. IEEE Transactions on Information Forensics and Security, 2009, 4(1): 123 - 139.

[50] KHANNA N, DELP E. Sensor forensics: Printers, cameras and scanners, they never lie [C]// Proceedings of 2007 IEEE International Conference on Multimedia and Expo. Washington, DC: IEEE Computer Society, 2007: 20 - 23.

[51] CELIKTUTAN O, SANKUR B, AVCIBAS I. Blind identification of source cell-phone model [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(3): 553 - 566.

[52] SWAMINATHAN A, WU M, LIU K J R. Nonintrusive component forensics of visual sensors using output images [C]// Proceedings of 2007 IEEE International Conference on Information Forensics and Security. Washington, DC: IEEE Signal Processing Society, 2007: 91 - 106.

[53] SWAMINATHAN A, WU M, LIU K J R. A pattern classification framework for theoretical analysis of component forensics [C]// 2008 IEEE International Conference on Acoustics, Speech and Signal Processing. Washington, DC: IEEE Computer Society, 2008: 1665 - 1668.

[54] IANEVA T, de VRIES A, ROHRIG H. Detecting cartoons: A case study in automatic video-genre classification [C]// Proceedings of 2003 IEEE International Conference on Multimedia and Expo. Baltimore, MD: IEEE Computer Society, 2003: 449 - 452.

[55] LYU S, FARID H. How realistic is photorealistic [J]. IEEE Transactions on Signal Processing, 2005, 53(2): 845 - 850.

[56] NG T, CHANG S F, HSU Y, *et al.* Physics-motivated features for distinguishing photographic images and computer graphics [C]// Proceedings of ACM Multimedia. New York: ACM Press, 2005: 239 - 248.

[57] WANG Y, MOULIN P. On discrimination between photorealistic and photographic images [C]// Proceedings of 2006 IEEE International Conference on Acoustics, Speech and Signal Processing. Toulouse, France: IEEE Signal Processing Society, 2006: II - II.

[58] 王玉平, 李生红, 赵峰, 等. 基于 AdaBoost 的计算机生成图像检测算法[J]. 计算机仿真, 2008, 25(7): 220 - 222.

[59] DIRIK A, BAYRAM S, SENCAR H, *et al.* New features to identify computer generated images [C]// Proceedings of 2007 IEEE International Conference on Image Processing. Washington, DC: IEEE Computer Society, 2007: IV-433 - IV-436.

[60] YU H, NG T, SUN Q. Recaptured photo detection using specularity distribution [C]// Proceedings of 2008 IEEE International Conference Image Processing. Washington, DC: IEEE Computer Society, 2008: 3140 - 3143.

[61] GLOE T, KIRCHNER M, WINKLER P, *et al.* Can we trust digital image forensics [C]// Proceedings of the 15th International Conference on Multimedia. New York: ACM Press, 2007: 78 - 86.

www.computerapplications.com.cn 计算机应用