基于模式噪声的手机图像篡改检测①

杨 弘, 周治平, 周翠娟

(江南大学 物联网工程学院, 无锡 214122)

摘 要: 模式噪声作为相机传感器的固有特征, 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. 因此基于模式噪声的多媒体取证已经被广泛应用在追溯图像来源检测中. 然而, 由于模式噪声的脆弱性, 容易被篡改者从一个相机复制到另一相机上. 针对这一问题, 首先对基于模式噪声的两种篡改方式进行研究, 并通过设定判定阈值进行篡改取证, 同时为了解决模式噪声的相关性检测过程中计算量大, 算法复杂度高等问题, 采用了改进的模式噪声集鉴别方式, 大大提高了篡改检测效率.

关键词: 手机相机; 被动认证; 模式噪声; 篡改检测; 小波去噪

Cell Phone Camera Image Tampering Detection Based on Pattern Noise

YANG Hong, ZHOU Zhi-Ping, ZHOU Cui-Juan

(School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, China)

Abstract: Sensor pattern noise has been proved to be an inherent fingerprint of digital cameras. Since the main component of it is independent of the environment, it is stable and widely exists in all sensor-based cameras. Therefore, it has been widely used in forgery detection of digital images. However, the sensor pattern noise is vulnerable and easily to be copied from one camera to another. To solve this problem, we first study the two tampering methods which based on sensor pattern noise, then set a determined threshold to realize forgery detection. Meanwhile, in order to settle the problems such as great calculation and high complexity of the algorithm among the correlation detection of sensor pattern noise, this paper introduces a method based on clustered pattern noise and improves the tamper detection efficiency in a large extent.

Key words: cell phone camera; passive authentication; sensor pattern noise; tamper detection; wavelet denoising

在当今的数字信息时代, 随着多媒体技术的迅速发展, 特别是手机的普及和手机摄像头的广泛使用, 人们获取数字图像也越来越简单方便. 据统计, 手机相机在手持设备中占据主要地位, 甚至已经超过了90%[1]. 虽然到目前为止手机相机的质量并不能与数码相机相媲美, 但手机相机的分辨率和图像质量的稳步提高使得与数码相机之间的技术差距不断缩小. 因此, 手机相机具有非常好的应用前景, 手机图像不仅在网上有广泛的传播, 甚至在很多新闻报纸上都已经采用手机图片进行消息传递. 与此同时, 由于一些图像编辑工具如 photoshop 的广泛应用, 使得手机图像的完整性和安全性被人们所质疑.

近年来, 国内外对基于数码相机的数字图像被动取证技术已经有了比较深入的研究, 而针对手机相机的研究还处于起始阶段. 表面上看, 手机相机与数码相机的成像管道相似, 但由于手机相机的价格、大小(包括传感器芯片和摄像头)、耗电量都只有数码相机的 1/10[2], 而正是由于手机相机的低质量和生产标准导致了它的强指纹特征, 这样更有利于被动取证工作的进行.

模式噪声作为图像固有水印用于相机源取证的方法最早由 J. Fridrich 提出[3], 它本质上是一种加性高斯白噪声模型随机的扩频信号, 可以被特定的滤波器检测到, 相比之前的鲁棒水印具有脆弱性. 当攻击者能获得来自某种相机的图像时, 它也可轻易估算出该相机的模式噪

① 收稿时间:2013-03-01;收到修改稿时间:2013-03-28

声, 并将其复制到任意其他图像中将其伪造成来自该相机的图像. 针对这一问题, Fridrich 提出了一种“三角系数”的方法[4,5], 将源相机参考噪声、源相机图像与测试图像分别设为三角形三个顶点, 通过计算三者之间的相关系数来判断测试图像是否被篡改, 但是该算法复杂度高, 不易进行. 本文在研究针对模式噪声的两种篡改方式实现过程的基础上, 通过阈值判断的方法进行取证, 简单有效, 提高了模式噪声作为相机指纹的安全性, 同时为了降低模式噪声相关性检测中的计算复杂度, 采用改进的模式噪声集鉴别方式, 进一步提高了篡改检测效率.

1 手机图像指纹

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, 因此本文沿用 Fridrich 的方法[6], 先将多幅原始图像通过小波滤波器滤去其低通滤波图像得到差值图像, 再将得到的插值图像进行叠加再求平均或采用最大似然估计法得到该手机相机的模式噪声. 本文所有的黑体字符都代表一个向量或矩阵, 通常而言, 采用一维索引代替二维索引对来实现矩阵的查找更加实用, 且能避免混淆. 对于某一图像 I, 其模式噪声可表示为:

$$W_I = I - F(I) = aIK + \theta \tag{1}$$

其中 F 表示滤波器; K 表示传感器的模式噪声系数, Θ 表示各类随机噪声的综合影响, 包括散粒噪声、读出噪声、数/模转换引起的量化噪声等; a 表示与 K 维数相同的衰减因子. 采用最大似然估计法计算模式噪声的系数 K 如下, 其中 $I_1, I_2, \cdots\cdots, I_N$ 表示来自同一相机的 N 幅图像.

$$K = \sum_{i=1}^{N} \frac{W_{I_i} I_i}{\sum_i^N (I_i)^2} \tag{2}$$

与之同时, 定义两幅图像 I 和 J 的相关系数如下:

$$corr(W_I, W_J) = \frac{(W_I - \overline{W_I}) \odot (W_J - \overline{W_J})}{\|W_I - \overline{W_I}\| \bullet \|W_J - \overline{W_J}\|} \tag{3}$$

其中, 矩阵运算符⊙定义为:$X \odot Y = \sum_{i=1}^{n} X[i]Y[i]$, $\overline{W_I}$ 和 $\overline{W_J}$ 分别表示 W_I 和 W_J 的像素均值.

同时, 为了解决模式噪声的相关性检测过程中计算量大, 效率低, 算法复杂度高等问题, 本文采用改进的模式噪声集鉴别方式, 大大降低算法的复杂度和计算量, 提高鉴别的效率. 具体的实现方法如下:

第一步: 将图像 I 通过低通滤波器得到残差图像 W, 并将其转化成一维数组形式, 按降序排列;

第二步: 将数组中的元素拆分为 N 个集合 $(W_1, W_2, \cdots\cdots W_N)$, 设定每个集合中元素的最大值与最小值不超过 $D_{\max}$, 并且元素的个数不少于 $N_{\min}$, 将尽可能多的元素归类;

第三步: 重复第二步操作直到所有的元素都已被归类为止.

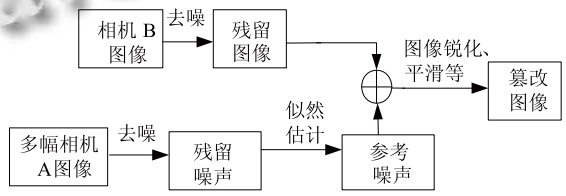
第四步: 将所得到所有集合中的 k 个集合 $(W_1, W_2, \cdots\cdots W_k)$ 作为图像 I 的模式噪声, 并与相机的参考噪声进行相关性计算.

通过设定 k 的值进行实验, 将实验结果进行对照, 选定一种误检率相对较小, 计算量较少的 k 取值方法作为最优方案.

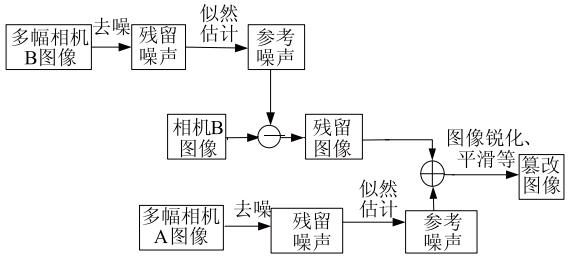
2 基于模式噪声的图像篡改方式

相比传统的鲁棒性水印, 模式噪声是一种比较脆弱的扩频信号, 能被特定的滤波器检测到, 对于技术娴熟的篡改者而言, 让它能成为篡改的对象并不困难. 本文主要研究一种称为“移花接木”的篡改方法.

首先, 我们假设这样一个情景: John 拥有一像素 500 万的手机 A, 将其拍摄的一组照片 $I_i(i = 1,2\cdots\cdots, N)$ 上传到自己的博客中与他人分享; 同时攻击者 Bob 也拥有一像素 500 万的手机 B, 并使用其拍摄了一组照片 $J_i(i = 1,2\cdots\cdots, N)$. 现在Bob从John的博客中得到图像 I_i, 并获得 A 手机相机的模式噪声 K_A, 他将模式噪声 K_A 加入到图像 J_i 中便可获得一组伪造图像用来陷害 John, 为了使篡改不露痕迹, 他试图在加入 K_A 之前先去掉本身的模式噪声, 通常有两种方式可以实现, 如图 1 所示:



(a) 篡改模型一



(b) 篡改模型二

图 1 两种篡改模型

由于相机模式噪声是一系列扩频信号, 在篡改过程中不可能全部滤去而不留一点痕迹, 本文通过实验对篡改前后的相关性分布进行对比, 并设定阈值对实验结果进行判断, 有效检测篡改行为.

为了对以上两种篡改方式做更多的研究, 本文使用 3 个相机分别拍 300 张照片进行实验, 针对每种相机使用其中的 100 张进行模式噪声提取, 并计算相机指纹之间的相关系数, 如果某一相机的照片与该相机之间相关性远比和其他相机高就能成功识别. 3 个相机的型号、分辨率等参数如下表 1 所示.

表 1　手机相机型号及其特性参数

	手机相机型号	分辨率	自动聚焦
A	Motorola Milestone	2592 ×1456	是
B	Nokia 6220c	2592×1944	是
C	Nokia 6700s	2592×1944	否

3　实验结果与分析

实验中选择 A 相机作为被攻击相机, B 相机为被篡改相机, C 相机为参考相机, 并设定 $D_{\max}=0.0025$, $N_{\min}=200$. 同时, 由多次实验证明选择 k 为总集合数 N 的 $\frac{1}{2}$ 能达到最佳效果. 首先, 将每个相机其中的 200 张照片与相机 A 进行相关性检测. 为了方便检测相机指纹间的相关性, 本文使用每张照片左上角的 1024×1024 区域作为检测区域. 实验结果如图 1 所示.

从图中可以看出, 相机 B、C 的源图像与相机 A 的指纹之间的模式噪声相关性远比相机 A 的照片与其本身的相关性弱. 为了探究图像被篡改前后的差别, 使效果更明显, 本文选择相机 B 的其中 10 张图像分别进行了如下实验, 首先将相机 A 的模式噪声直接复制到相机 B 的 10 张图像中, 为了方便区分称其为粗篡改, 并检测它们与相机 A、B、C 之间的相关系数, 结果如图 2 所示.

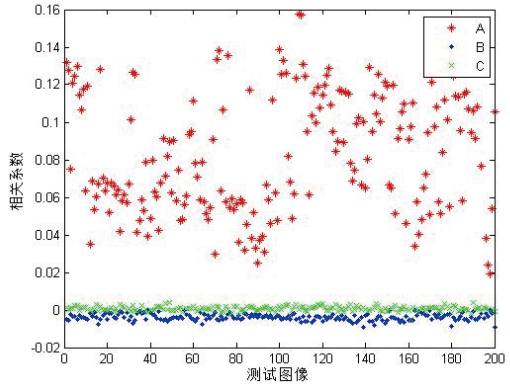


图 2　样本图像与相机 A 模式噪声之间的相关系数分布

从图 2 可以看出, 篡改后的图像与相机 A、B 之间的相关系数差距缩小, 已无法分辨. 同时, 这也意味着这些图像并不一定出自相机 A, 因此, 要进一步处理, 我们分别对两种篡改方式进行实验, 将之前的 10 张照片先滤去本身的模式噪声, 在得到的残留图像上加上相机 A 的模式噪声, 并进行相关性检测, 结果分别如图 3、4 所示.

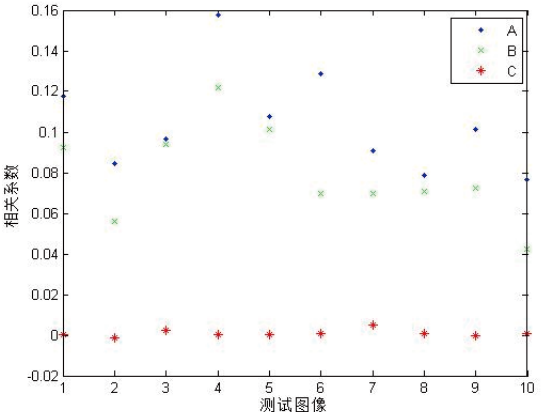


图 3　粗篡改后的图像与相机 A、B、C 之间的相关系数

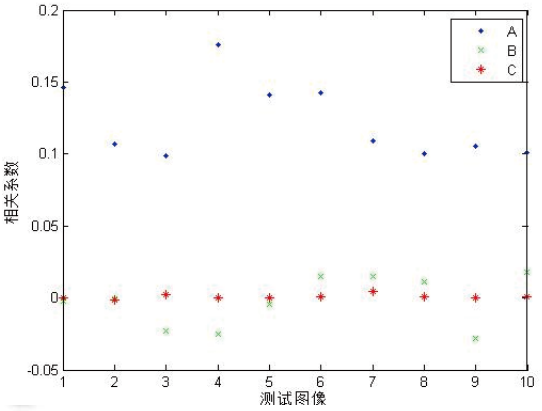


图 4　图像采用第一种篡改方式后与相机 A、B、C 之间的相关系数

从图 3、4 可以看出, 在篡改过程中先去掉本图像或本相机的模式噪声都能避免有两个相关系数的峰值, 然而, 图 3、4 也反映了图像被篡改之后与相机 B 之间的相关性较相机 C 波动比较明显, 将其与图 1 相比便可从一些细微迹象表明图像有被篡改的可能. 另外, 图 3 中篡改图像与相机 A 的相关系数均值比图 1 中相机 A 与其本身图像之间的相关系数大得多, 这也是暗示之一.

然而, 以上判断仅是基于对实验结果的直观判断, 并不能形成理论, 在此基础上, 本文根据篡改图像与

相机 B 之间相关系数特征, 设定相关系数方差判定阈值 t, 通过大量的实验确定本文的 t 值为10^{-5}. 若δ^2大于 t, 则判定图像为篡改图像, 反之亦然.

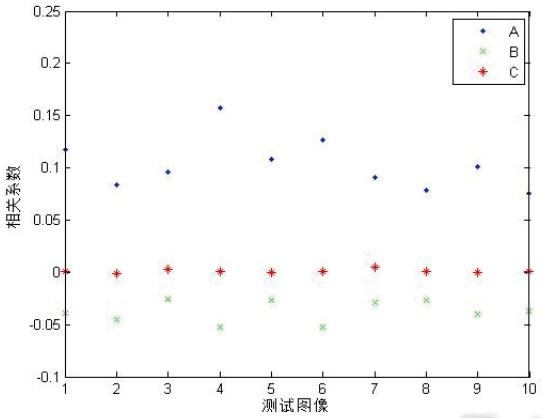


图 5 图像采用第二种篡改方式后与相机 A、B、C 之间的相关系数

计算结果显示, 图 4 中图像与相机 B 之间的相关系数方差δ^2为3.11×10^{-4}, 而图 5 中δ^2为5.39×10^{-4}, 均大于 t, 故判断图 4、5 中的图像为篡改图像.

5 总结

模式噪声作为相机指纹的脆弱性和易被拷贝、篡改, 手机相机作为当前使用最广泛的手持设备, 加上它与数码相机相比具有的低质量和低生产标准, 而成为本文研究的主要对象. 本文在研究针对模式噪声的两种篡改方式实现原理和过程的基础上, 通过阈值判断的方法进行取证, 简单有效, 提高了模式噪声作为相机指纹的安全性, 同时为了降低模式噪声相关性检测中的计算复杂度, 采用改进的模式噪声集鉴别方式, 进一步提高了篡改检测效率.

参考文献

1 Cao H, Kot AC. Mobile camera identification using demosaicing features. 2010 IEEE International Symposium on Circuits and Systems: Nano-Bio Circuit Fabrics and Systems, ISCAS 2010. United States: IEEE Computer Society, 445 Hoes Lane, 2010: 1683–1686.

2 Cao H, Kot AC. Detection of tampering inconsistencies on mobile photos. Digital watermarking-9th international workshop,IWDW 2010,revised selected papers. Germany: Springer Verlag, Heidelberg, 2011: 05–119.

3 Fridrich J, Lukas J, Goljan M. Digital Camera Identification from Sensor Noise. IEEE Transactions on Information Security and Forensics,2006:1–2.

4 Miroslav G, Jessica F, Chen M. Defending against fingerprint-copy attack in sensor-based camera identification. IEEE Transactions on Information Forensics and Security. 2011,6(1):227–236.

5 Fridrich J, Chen M, Goljan M. Digital Imaging Sensor Identification. Proc.of SPIE Electronic Imaging, Photonics West, January 2007. 16–19.

6 Yoichi T, Hitoshi K. Digital camera identification based on the clustered pattern noise of image sensors. 2011 IEEE International Conference on: Multimedia and Expo(ICME). 2011,9(6):1–4.

7 袁秀娟,黄添强,陈智文,吴铁浩,苏立超.基于纹理特征的数字视频篡改检测.计算机系统应用,2012,21(6):91–95,152.

8 Li CT, Chang CY, Li Y. On the Repudiability of Device Identification and Image Integrity Verification Using Sensor Pattern Noise. Weerasinghe D. Information Security and Digital Forensics. Springer Berlin Heidelberg, 2010: 19–25.

9 Martin Steinebach,Liu,Huajian,Fan,Peishuai,Katzenbeisser, Stefan.Cell Phone Camera Ballistics:Attacks and Counterm-easures SPIE Conference on Multimedia on Mobile Devices.City.

10 Steinebach M, Ouariachi M, Liu HJ, Katzenbeisser S. On the Reliability of Cell Phone Camera Fingerprint Recognition. Goel S. Digital Forensics and Cyber Crime. Springer Berlin Heidelberg, 2010:69–76.