基于 BAG 误匹配的 JPEG 窜改图像的被动检测算法*

张 鑫, 周尚波
(重庆大学 计算机学院, 重庆 400044)

摘 要: 当 JPEG 图像被窜改时,通过检测人工的块状网格 BAG(block artifact grid)误匹配的痕迹,可以判定待检测图像是否被窜改过,但这种算法有较高的虚警率,提出一种改进算法。首先利用 BAG 误匹配原理检测图像,再在疑似窜改区域检测竖直方向和水平方向上是否同时存在相邻 BAG 的边缘,从而将窜改区域与偶发噪声点区域分开,最后对全图进行形态学处理,进一步消除噪声。实验证明,该算法可以在有效检测窜改区域的情况下,降低算法的虚警率,在数字图像的被动检测领域有广泛的应用前景。

关键词: JPEG 图像; 人工块状网格; 窜改; 虚警率; 被动检测
中图分类号: TP391 **文献标志码**: A **文章编号**: 1001-3695(2012)12-4626-05
doi:10.3969/j.issn.1001-3695.2012.12.057

Passive detection of doctored JPEG image via BAG mismatching

ZHANG Xin, ZHOU Shang-bo
(*College of Computer Science*, *Chongqing University*, *Chongqing* 400044, *China*)

Abstract: When JPEG image is tampered with, researchers could distinguish a detected image which may be changed or not according to the trace of BAG mismatching. But this algorithm produce high false alarm rate. This paper proposed a method which could improve original algorithm. Firstly, it detected an image based on the principle of BAG mismatching. Secondly, it could make use of the edge of adjacent BAG in vertical and horizontal direction to make a distinction between doctored region and accidental noisy point in doubtful region of the image. Finally, in order to reduce more noise, morphology processing was performed on the image. The experiment demonstrates that the algorithm can lower false alarm rate with effective detection and will be applied widely in the region of passive detection of digital image.

Key words: JPEG image; BAG; distortion; false alarm rate; passive detection

0 引言

随着电脑硬件和软件的快速发展,现代信息社会已经可以令非专业人员进行原本复杂的数字图像处理,几乎任何人员都可以以极小的成本获得被窜改的高质量的数字图像。这就使得人们对图像的真实性产生了怀疑,这种怀疑的氛围不仅给人们的生活造成了种种的不方便,而且破坏了社会的诚信,提高了社会管理的成本。为了解决愈演愈烈的窜改图像的风潮,现在迫切需要一个可靠的能够鉴别数字图像真伪的自动识别系统。这种识别系统将会在法院调查、犯罪物证识别、智能服务、医学图像识别等众多社会领域中发挥重要的作用。

在目前检测数字图像窜改的理论中主要被分成主动检测技术和被动检测技术两类。主动检测技术[1]的窜改认证是通过检测图像中的数字水印或数字签名来判断图像是否被修改过。这种技术需要图像预先嵌入数字水印或签名,而这个条件限制了主动鉴别技术的应用,因为现实生活中的大部分数字图片并没有预先嵌入可供检测的信息。被动检测技术是一种新型的图像检测方式,它与主动检测的技术相反,不需要任何预先嵌入到图像中的信息,因此被动检测会遭遇到很多技术难题,针对这些难题研究人员也设计了很多方法[2]。被动检测技术可以根据窜改图像时的一些特征进行检测,如特征向量的相似度匹配[3~7]、图像的边缘特征[8]等多种方法进行检测。

JPEG 格式的图像应用十分广泛,尤其是在数码相机所拍摄的照片中。因为 JPEG 格式是一种有损压缩格式,能够将图像压缩在很小的储存空间。图像中重复或不重要的资料会丢失,容易造成图像数据的损伤。因此上述算法通常只能应用于无压缩或者具有较高质量的图片中,很难应对有图像数据丢失的 JPEG 格式图像。最近几年来研究人员也提出了很多专门针对 JPEG 图像窜改的检测方式,利用 JPEG 图像所特有的一些特征进行检测。在 JPEG 图像压缩过程中,图像会引入一些人工插入点来平衡压缩率和图像质量。当对 JPEG 格式的图像进行窜改时,这些插入点会保留下窜改的痕迹,可用来检测图像的真实性。将图片分成固定大小的图像块,将每一个图像块的 DCT 系数作为图像块的特征向量进行

收稿日期: 2012-05-18; **修回日期**: 2012-06-30 **基金项目**: 国家自然科学基金资助项目(60873200;61004112); 211 工程第 3 期资助项目(S-10218)

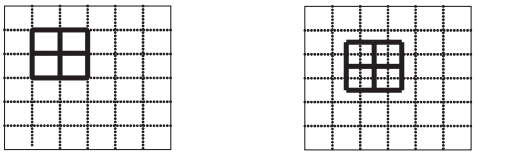
作者简介: 张鑫(1988-),男,山西长治人,硕士研究生,主要研究方向为图像处理(zxb06521@163.com);周尚波(1963-),男,广西宁明人,教授,博士,主要研究方向为混沌及其控制理论、图像处理、信息安全、物理工程计算及计算机仿真技术等.

相似度匹配[9]。但是这个算法具有较高的时间复杂度,并且通常只能针对 copy-move 窜改图像的方式。利用最大似然估计的方法来估计 JPEG 图像的量化矩阵,并通过量化矩阵来检测图像的真实性[10,11]。但是这种算法不仅会出现由局部最小值产生的虚警区域,而且还具有较高的时间复杂度。文献[12]提出了基于 DCT 系数的直方图功率谱来估计量化矩阵,可以减少时间复杂度。文献[13]通过估计量化的 DCT 系数的直方图的周期来估计量化矩阵中的量化步,并将每一个可能量化步的协方差和最小期望值结合来滤除局部最小值。另外一种检测方法是利用 BAG (block artifact grid)。当进行窜改图像的操作时,窜改区域的 BAG 会跟随窜改区域一起移动,并且通常会与原始图像中的 BAG 产生误匹配。通过提取出 JPEG 格式图像中的 BAG,然后再根据检测误匹配来定位出图像中的窜改区域[14]。文献[15]也是基于提取 BAG,再检测 BAG 误匹配来定位窜改区域的,但是其提供了一种新的提取和标记误匹配区域的方法。利用 BAG 误匹配来检测图像的真实性具有很多优良的性质,对于多种窜改方式(旋转、copy-move、拼接、加噪)均具有较好的检测效果,并且具有较低的时间复杂度。但是这种算法也有其局限性,其中一个限制条件就是对于具有强边缘或高频特征的图像,利用人工块状网格 BAG 的算法来检测会出现很多虚警的区域,从而严重影响窜改区域的识别。

1　基于 BAG 误匹配的自动检测和定位算法

1.1　BAG 误匹配

在引言中提出了 BAG 的概念,本章将对 BAG 误匹配给出详细的解释。对于使用非常广泛的 JPEG 格式图像,在压缩图像的过程中,会产生间隔点,这些点就组成了垂直和水平的网格线,这就是 BAG。在 JPEG 格式的图像中通常有两种噪声:a)自然噪声,这是一种随机噪声,通常此类噪声非常弱;b)BAG 噪声,此种噪声在垂直和水平方向的周期为 8 个像素点。BAG 现象是 JPEG 格式的图像所独有的特征。在图 1 中,每一个网格代表一个 8×8 个像素的图像块,虚线所形成的网格代表的就是图像中的 BAG。粗线条所构成的区域就是窜改图像时所用到的区域。图 1(a)是原始图像,(b)是窜改后在 BAG 的位置变化情况。在图 1(b)中可以清楚地看到,来自于窜改区域的 BAG 与原始图像中的 BAG 并没有重合,发生误匹配。



(a) 原始图像的BAG　　(b) 图像窜改后的BAG误匹配

图1　BAG误匹配

每一个网格代表 8×8 像素的图像块,当图像块不发生旋转时 BAG 错误匹配的概率是 $1-1/8^2=98.4375\%$;当发生旋转时不仅要求网格匹配,还要求旋转角度只能是 0°、90°、180°、270°,所以旋转窜改区域时发生 BAG 错误匹配的概率会更高。当然以上仅是理论上的分析,由于图片千差万别,任何算法在应用过程中都会或多或少地出现一些噪声,所以即使是针对同样理论设想,不同算法的检测效果也不同。

1.2　BAG 自动提取算法

BAG 信号在 JPEG 格式中非常弱,提取时可以考虑首先采用二阶微分的绝对值。因为一阶微分产生较粗的边缘,而二阶微分则细得多,所以可以预料在进行边缘增强处理时二阶微分比一阶微分的效果强。在式(1)(2)中,$f(x,y)$是图像中像素值,x 是像素点的横坐标值,y 是像素点的纵坐标值,$f_v(x,y)$是垂直方向上的二阶微分值,$f_h(x,y)$是水平方向上的二阶微分值。

$$f_v(x,y)=|2f(x,y)-f(x,y-1)-f(x,y+1)| \tag{1}$$

$$f_h(x,y)=|2f(x,y)-f(x-1,y)-f(x+1,y)| \tag{2}$$

由于算法中提取 BAG 中水平线和垂直线的过程是相似的,所以仅介绍提取水平方向的 BAG 信号算法过程。在图像中经常会出现使二阶微分值很大的强边缘,如细线和孤立点,这种情况对于提取 BAG 都是噪声点,会产生干扰。为了弱化干扰和降低虚警率,可以将 $f_h(x,y)$最大值定为 50。在图像中 BAG 信号很弱,因此可以通过累加和的方式加强信号强度。

$$M(x,y)=\sum_{i=x-16}^{x+16} f_v(i,y) \tag{3}$$

在算法中选择 $f_v(x,y)$一个像素点水平方向上左右各 16 个像素点的像素值进行累加来增强信号强度。若选择累加的像素点个数较少,则信号强度不够;若选择累加的像素点个数较多,则会增加噪声出现的概率。水平方向上左右各有两个网格中的点进行累加,较好地平衡了两方面的因素。因为在图像中既存在二阶微分值较大的强边缘,又存在二阶微分值很小的平坦区域,如大片的草地、蓝天等。而 BAG 信号强度常常介于这两种情况的微分值之间。为了在增强 BAG 水平方向信号强度的情况下弱化噪声的影响,还需要应用中值滤波器。

$$M_h(x,y)=M(x,y)-\mathrm{Mid}[\{M(x,i)\,|\,y-16\leqslant i\leqslant y+16\}] \tag{4}$$

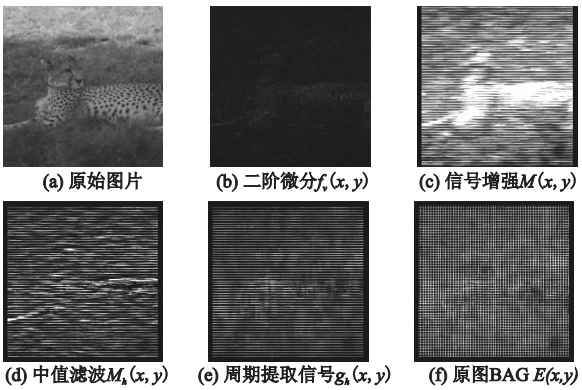
BAG 信号只会出现在网格的边缘,在水平和垂直方向都是周期信号,并且强度值介于图像灰度级阶梯变化快的强边缘区域和灰度级阶梯变化慢的平坦区域的二阶微分值之间,所以可以利用周期性质和信号强度的性质进行提取。

$$g_h(x,y)=\mathrm{Mid}[\{M_h(x,i)\,|\,i=y-16,y-8,y,y+8,y+16\}] \tag{5}$$

提取垂直方向上的 BAG 信号与上述过程类似,最后 JPEG 格式图像的 BAG 信号由水平方向和垂直方向相加而成。

$$E(x,y)=g_h(x,y)+g_v(x,y) \tag{6}$$

图 2 是质量因子 $q=40$ 的一张没有被窜改过的图片应用上述方法提取 BAG 的过程。



(a) 原始图片　(b) 二阶微分$f_v(x,y)$　(c) 信号增强$M(x,y)$

(d) 中值滤波$M_h(x,y)$　(e) 周期提取信号$g_h(x,y)$　(f) 原图BAG $E(x,y)$

图2　提取BAG过程

1.3 窜改区域自动定位算法

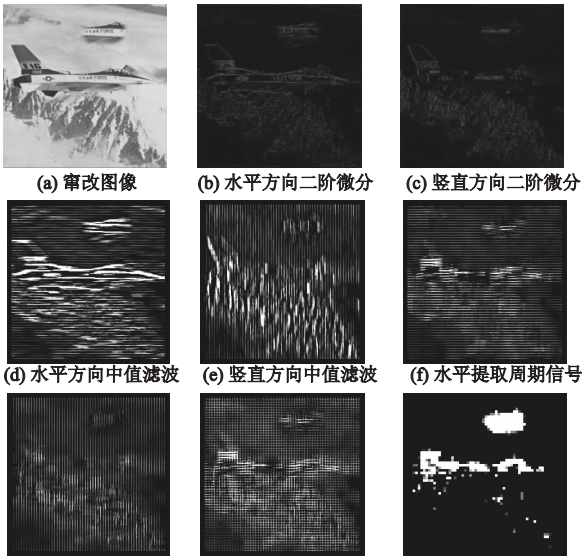
在成功提取图片的 BAG 后,可以看到在一张未被窜改过的 JPEG 格式图片中只有 8 × 8 网格的边缘部分像素值较高,网格内部的像素值通常很低。根据前面介绍的 BAG 误匹配的相关内容,可以联想到若发生 BAG 误匹配后,被窜改区域的网格就会有错位的现象,此时网格内也会出现像素值高的点,因此可以利用这个特点制定自动定位窜改区域的方法。以一个 BAG 网格 N 为例,网格内有像素点 36 个,边缘有像素点 28 个。$N(x,y)$ 表示网格中横坐标为 x、纵坐标为 y 的像素。

$$a = \max\{\sum_{i=2}^{7} N(x,i) \mid 2 \leqslant x \leqslant 7\} + \max\{\sum_{i=2}^{7} N(i,y) \mid 2 \leqslant y \leqslant 7\} - \min\{\sum_{i=2}^{7} N(i,y) \mid y = 1,8\} - \min\{\sum_{i=2}^{7} N(x,i) \mid x = 1,8\} \quad (7)$$

2 基于 BAG 误匹配的改进算法

2.1 BAG 误匹配算法的缺陷

由于图像的复杂和多样性,以及每一种算法都不可避免的局限性,BAG 误匹配算法的应用还有一些限制条件。实验发现,以上算法对于带有强边缘的图像具有较高的虚警率,严重干扰了人们对于窜改区域的判断。图 3 将通过一个实例揭示产生虚警的原因。



(a) 窜改图像 (b) 水平方向二阶微分 (c) 竖直方向二阶微分

(d) 水平方向中值滤波 (e) 竖直方向中值滤波 (f) 水平提取周期信号

(g) 竖直提取周期信号 (h) 窜改图像BAG (i) 窜改区域定位

图3 强边缘图像产生虚警的原因分析

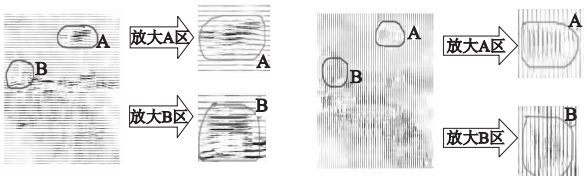
图 3(a)是质量因子 $q = 30$ 的原始图像在经过窜改后保存为质量因子 $q = 90$ 的窜改图像,窜改区域是将图像中飞机的一部分复制粘贴到图像的右上角。在图中可以明显看到飞机与图像背景的边界具有强烈的对比度。通过图 3(b)(c)中的二阶微分结果可明显看到飞机的轮廓边缘。由于存在强边缘情况,在经过信号增强后会出现大片像素值较高的区域。即便是经过噪声弱化和利用周期性质过滤后仍然无法去除强边缘附近的亮区域,如图 3(d) ~ (g)。导致的结果是在未窜改的区域内会出现像素值较高的“亮点”。因此在这些区域内虽然不是窜改的区域,但是在 8 × 8 的网格内部也会出现很多像素值较高的亮点。这也是应用上文的窜改区域自动定位算法会出现较高虚警率的最重要的原因。如图 3(i)中,在成功定位出窜改区域的同时,也在原始图像飞机的区域中出现了很多错误的检测结果。

所以需要对 BAG 误匹配算法进行改进,使得能够在成功定位出窜改区域的同时,尽量减少算法的虚警率。

2.2 BAG 误匹配算法缺陷的深入探讨

为了既能检测出窜改区域,又能够消减、降低虚警率,需要找出窜改区域和非窜改区域的不同,从而找到差异加以区分。为了更加清晰地看到图像中的差异,将图像进行了反色处理。

在图 4 中分别展示出 $g_h(x,y)$ 和 $g_v(x,y)$ 的反色图。图中所标志的 A 区域和 B 区域分别是窜改区域和非窜改区域中产生虚警的区域,并且分别将这两个区域的放大图呈现出来。经过仔细观察,在图 4(a)(b)右侧两个小图中可看到,在窜改区域 A 中的水平方向和竖直方向上同时存在紧密相连的黑色区域。如在(a)中水平方向上除了以 8 为周期的水平线外,在周期性的水平线内部还有黑色区域,并且黑色区域并不是在水平方向上仅有一条黑色线段,而是至少在竖直方向上有相邻的两条黑色线段;在图(b)中除了以 8 为周期的竖直线段外,在其内部也存在水平方向上相邻的黑色线段。再观察 B 区域中水平方向和竖直方向的放大图,可以看到在两个方向上除了以 8 为周期的网格线内部虽然也有黑色的线段,但是很少存在相邻的线段,大多是孤立的一条线或若干个点,即便在一个方向上存在一片相邻的黑色区域,但在另一个方向上的同一个区域也不会存在相邻的黑色区域。



(a) 图3中$g_h(x,y)$反色图及A和B两区域对比 (b) 图3中$g_v(x,y)$反色图及A和B两区域对比

图4 强边缘图像产生虚警的原因分析

经过观察得出窜改区域 A 和非窜改区域中产生虚警的区域 B 的一个重要差别。为了设计区分算法,还需要探讨关于产生这一重要差异的原因。B 中产生黑色线段的原因是在原图像中所对应的区域具有强边缘,在经过弱化和周期性过滤后仍然难以去掉。但是在一个区域边缘通常只会向一个方向延伸,所以即便在一个方向上出现黑色区域,在另一个方向上的同一个区域也几乎不会出现黑色区域。并且在 B 区域中由于图像边缘的随机性,即使在一些区域出现黑色线条或若干个黑点,但也几乎不会出现空间上相邻的线条。

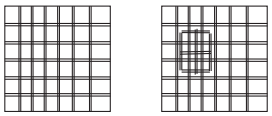
在窜改区域 A 中以 8 为周期的黑色线条之间的黑色区域部分并不像 B 区域一样,不仅在两个方向上都存在,而且在空间上具有相邻的特点。分析产生这种现象的原因,回顾算法的理论基础,发现是由于 BAG 误匹配来检测窜改区域的,而误匹配正是由于边界的不重合造成的。

如图 5 所示。重新考察 BAG 网格,发现由于大小为 8 × 8 个像素的图像块是彼此相邻的,一个图像块的边线和相邻的图像块的边线在空间上是相邻的。因此在图 5(a)中可以看到,两个相邻图像块的边线在空间上是相邻的。当发生 BAG 误匹配时,图像块的边界就会产生错位。在图 5(b)中可以看到,在误匹配区域,发生错位的并不是一条边界线,而是相邻的两个图像块的边界线都会发生误匹配。这就可以解释在窜改区域中水平和竖直方向上都存在空间位置上相邻的两条亮线。

在发现了窜改区域和非窜改区域中发生虚警区域之间的差异并了解产生差异的原因后,可以知道这种差异并不是偶然现象,而是基于 BAG 算法误匹配理论所产生的必然结果。由此可以利用这种差异将两个区域区分开来。

2.3　BAG 误匹配算法改进

本文设计的改进算法,是在 BAG 误匹配算法后加入去噪环节,而去噪算法的理论基础就是上节所述的差异。具体算法流程如图 6 所示。



(a) 未窜改区域BAG　(b) 窜改区域的BAG

图5　BAG网格示意图

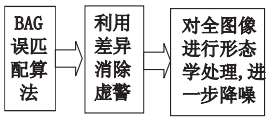


图6　BAG误匹配改进算法

BAG 误匹配算法前文已经详述,不再讨论。在上节中已经详述了窜改区域和非窜改区域中发生虚警区域之间差异的原因。因此在利用差异消除虚警时可以采用以下方法:

a)利用式(7)对图中每一个 8×8 图像块进行计算,若大于 0,则进入下一步;否则退出。

b)对值大于 0 的图像块将水平和竖直方向相结合进行比较。在一个方向上除了边界 2 个点外,内部还有 6 个点。若这 6 个点中有 4 个点的像素值大于 10,则可以认为是一条亮线,同时记录下此亮线的位置。

c)若图像块中同时满足在水平和竖直方向上都存在两条相邻的亮线,则认定此区域为窜改区域,而不是虚警区域。并利用步骤 a)中式(7)计算的值对属于窜改区域中图像块的像素进行赋值。

最后对全图进行形态学处理,进一步消除一些偶发噪声,从而突出窜改区域。首先进行图像的二值化处理,对于值大于 15 的像素设为 255,其余像素值设为 0。然后消除孤立噪声点,在此过程中以相邻 3×3 个 8×8 大小的图像块为模板遍历整个图像。在模板中若只有一个图像块中像素的值为 255,其余八个值均为 0,则认为此图像块为噪声,并将其中像素设为 0。最后采用闭运算来填充细小空洞,连接邻近物体,平滑边界,同时不明显改变目标图像的面积。

经过上述改进,再次进行实验的结果如图 7 所示。

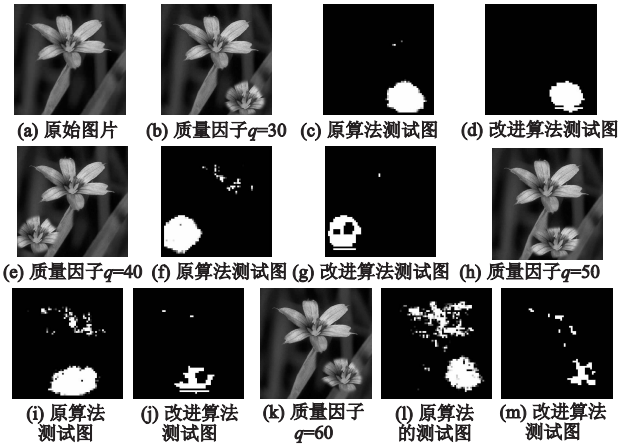
(a) 窜改图像　(b) 改进算法后实验结果

图7　改进算法实验结果

从图 7 可以清晰地看到,在能够有效检测到窜改区域的情况下,噪声区域已经大幅度地减少,并且噪声图像块的面积比窜改区域图像块的面积小很多,基本不影响对窜改区域的定位。

2.4　算法改进实验及实验结果分析

在本实验中首先随机选取 120 幅图片,对每一幅图片都分别进行实验前预处理。将图片分别复制 4 幅并将窜改前图片的质量因子 q 分别设为 30、40、50、60。窜改后再全部保存为质量因子 $q=90$ 的窜改图片。实验环境是 VC++6.0 与 OPENCV1.0,AMD Athlon™ Ⅱ X2 250 3.00 GHz CPU,4 GB 内存。实验过程中的窜改图片和实验结果图片如图 8 所示。



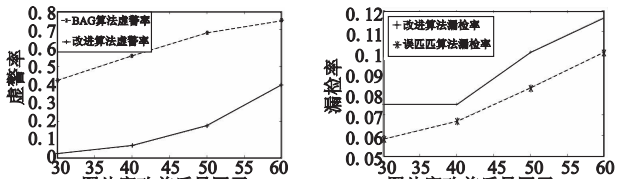
(a) 原始图片　(b) 质量因子q=30　(c) 原算法测试图　(d) 改进算法测试图

(e) 质量因子q=40　(f) 原算法测试图　(g) 改进算法测试图　(h) 质量因子q=50

(i) 原算法测试图　(j) 改进算法测试图　(k) 质量因子q=60　(l) 原算法的测试图　(m) 改进算法测试图

图8　实验图片及两算法效果对比

从上述实验的测试结果中可以看到,不论是原 BAG 误匹配算法还是改进算法,随着质量因子 q 的增加,噪声形成的虚警区域逐渐增加。然而在原算法中虚警区域增加非常快,当质量因子达到 $q=50$ 和 $q=60$ 时虚警区域已经比较多,尤其是在最后一组 $q=60$ 的实验中,虚警区域已经严重干扰了对于窜改区域的定位。但是从每组实验的两个对比中可以发现,改进算法中的虚警区域要明显少于原算法,并且可以比较容易地定位出窜改区域,因为标记窜改区域的白色像素块的面积要明显大于虚警区域。由此可见,改进算法可以实现在有效监测窜改区域的前提下,较大幅度地减少虚警的区域,从而有利于窜改区域的定位。对 120 幅图片进行上述实验,实验结果统计如图 9 所示。



(a) BAG误匹配算法与改进算法虚警率对比　(b) BAG误匹配算法与改进算法漏检率对比

图9　BAG误匹配算法与改进算法虚警率和漏检率对比

实验中为了比较两个算法的实验效果,引入虚警率和漏检率两种测试量。虚警率为虚警区域影响到窜改区域定位的图片与所有图片的比值。漏检率为实验中没有检测到窜改区域的图片与所有图片的比值。从图 9(a)中可以看到,随着质量因子的增加,实验中虚警率也会随之增加,但对同一个质量因子,改进算法的虚警率比原始 BAG 误匹配算法有明显的降低。四组实验改进算法的虚警率平均值为 16.675%,比原算法平均值降低了 41.2325%,以上数据说明改进算法在降低虚警率方面比原算法更加有效。从图 9(b)中可以看到,两个算法的漏检率曲线走势也是随着质量因子 q 的增加而增加。四组实验中改进算法对应的漏检率平均值约为 9.17%,只比原算法平均值上升了 1.46%,基本上与原 BAG 误匹配算法的漏检率相等,而且从实际应用来看,10% 左右的虚警率也是可以接受的。从图 9 中可以看到,对 BAG 误匹配算法的改进是成功的,在保留窜改区域的前提下,虚警率有了大幅度的降低。

3 结束语

被动检测在实际生活中应用范围很广,成为近年来图像领域的热点。针对 JPEG 格式图像的被动检测有很多算法,每一种算法都有其优势和局限性,BAG 误匹配算法有其独特的优势,其能够检测多种窜改类型,如 copy_move、拼接、旋转、加噪声等,但是其较高的虚警率让其应用范围和检测效果都难以令人满意。因此,对于 BAG 误匹配算法的改进就很重要。在保证该算法仍然具有优良的检测窜改区域的性能的同时,尽可能地减少虚警区域是一个非常重要的改进方向。另外,在检测时该算法要求图片窜改前的质量因子要小于窜改后保存图片时的质量因子,并且两质量因子差值越大,检测效果越好;若质量因子差值较小,通常虚警率就会上升,影响检测效果,因此这将是此算法今后的一个改进方向。

参考文献:

[1] REY C, DUGELAY J. A survey of watermarking algorithms for image authentication [J]. EURASIP Journal on Advances in Signal Processing, 2002, 2002(6): 613-621.

[2] GRANTY R E J, ADITYA T S, MADHU S S. Survey on passive methods of image tampering detection [C]//Proc of International Conference on Communication and Computational Intelligence. [S. l.]: IEEE Computer Society, 2010: 431-436.

[3] 骆伟祺,黄继武,丘国平. 鲁棒的区域复制图像窜改检测技术[J]. 计算机学报, 2007, 30(11): 112-121.

[4] MAHDIAN B, SAIC S. Detection of copy-move forgery using a method based on blur moment invariants [J]. Forensic Science International, 2007, 171(2): 180-189.

[5] KANG Li, CHEN Xiao-ping. Copy-move forgery detection in digital image[C]//Proc of the 3rd International Congress on Image and Signal Processing. [S. l.]: IEEE Computer Society, 2010: 2419-2421.

[6] 康晓兵,魏生民. 基于 TSVD 的图像复制区域伪造检测算法[J]. 计算机应用研究, 2008, 25(12): 227-229.

[7] 康晓兵,魏生民. 一种基于自适应阈值的图像伪造检测算法[J]. 计算机应用研究, 2011, 38(3): 301-305.

[8] ZHANG Zhen, ZHANG Pei-ying, YU Zhou. A novel approach for detecting forged image[C]//Proc of the 5th IEEE International Conference on Bio-Inspired Computing: Theories and Applications. [S. l.]: IEEE Computer Society, 2010: 958-961.

[9] HUANG Yan-ping, LU Wei, SUN Wei. Improved DCT-based detection of copy-move forgery in images[J]. Forensic Science International, 2011, 206(1): 178-184.

[10] FRIDRICH J, GOLJAN M, DU R. Steganalysis based on JPEG compatibility[C]//Proc of Multimedia Systems and Applications IV. [S. l.]: SPIE, 2001: 275-280.

[11] FAN Zhi-qiang, De QUEIROZ R L. Identification of bitmap compression history: JPEG detection and quantizer estimation [J]. IEEE Trans on Image Processing, 2003, 12(2): 230-235.

[12] YE Shui-ming, SUN Qi-bin, CHANG Ee-chien. Detecting digital image forgeries by measuring inconsistencies of blocking artifact[C]// Proc of IEEE International Conference on Multimedia and Expo. [S. l.]: IEEE Computer Society, 2007: 12-15.

[13] WANG Zhong-mei, LONG Yong-hong. Digital image forgeries detection based on blocking artifact[C]//Proc of IEEE Conference on Information, Computing and Telecommunications. [S. l.]: IEEE Computer Society, 2010: 255-258.

[14] LI Wei-hai, YUAN Yuan, YU Neng-hai. Doctored JPEG image detection[C]//Proc of IEEE International Conference on Multimedia and Expo. [S. l.]: IEEE Computer Society, 2008: 253-256.

[15] LI Wei-hai, YUAN Yuan, YU Neng-hai. Passive detection of doctored JPEG image via block artifact grid extraction[J]. Singal Processing, 2009, 89(9): 1821-1829.

(上接第 4625 页)

[5] LI Ji-guo, HUANG Xin-yi, MU Yi, *et al*. Certificate-based signature: security model and efficient construction[C]//Lecture Notes in Computer Science, Vol 4582. Berlin: Springer-Verlag, 2007: 110-125.

[6] LIU J K, BAEK J, SUSILO W, *et al*. Certificate-based signature schemes without pairings or random oracles[C]//Lecture Notes in Computer Science, Vol 5222. Berlin: Springer-Verlag, 2008: 285-297 .

[7] WU Wei, MU Yi, SUSILO W, *et al*. Certificate-based signatures revisited[J]. Journal of Universal Computer Science, 2009, 15(8): 1659-1684.

[8] HUANG Xin-yi, MU Yi, SUSILO W, *et al*. Certificateless signature revisited [C]//Lecture Notes in Computer Science, Vol 4586. Berlin: Springer-Verlag, 2007: 308-322.

[9] AU M H, LIU J K, SUSILO W, *et al*. Certificate based(linkable) ring signature[C]//Lecture Notes in Computer Science, Vol 4464. Berlin: Springer-Verlag, 2007: 79-92.

[10] WANG Li-hua, SHAO Jun, CAO Zhen-fu, *et al*. A certificate-based proxy cryptosystem with revocable proxy decryption power[C]// Lecture Notes in Computer Science, Vol 4859. Berlin: Springer-Verlag, 2007: 297-311.

[11] SHAO Zu-hua. Certificate-based fair exchange protocol of signatures from pairings[J]. Computer Networks, 2008, 52(16): 3075-3084.

[12] CHAUM D. Blind signature for untraceable payments[C]//Proc of Advances in Cryptology-CRYPTO. Berlin: Plenum Press, 1983: 199-233.

[13] HARA Y, SEITO T, SHIKATA J, *et al*. Unconditionally secure blind signatures[C]//Lecture Notes in Computer Science, Vol 4883. Berlin: Springer-Verlag, 2009: 23-43.

[14] 周萍, 何大可. 高效无可信 PKG 的新型盲签名方案[J]. 计算机应用研究, 2012, 29(2): 626-629.

[15] BARRETO P S L M, LIBERT B, MCCULLAGH N, *et al*. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]//Lecture Notes in Computer Science, Vol 3778. Berlin: Springer-Verlag, 2005: 515-532.

[16] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[17] BONEH D, BOYEN X. Short signatures without random oracles [C]//Lecture Notes in Computer Science, Vol 3027. Berlin: Springer-Verlag, 2004: 56-73.

[18] FISCHLIN M, SCHRÖDER D. On the impossibility of three-move blind signature schemes [C]//Lecture Notes in Computer Science, Vol 6110. Berlin: Springer-Verlag, 2010: 197-215.

[19] HE De-biao, CHEN Jian-hua, ZHANG Rui. An efficient identity-based blind signature scheme without bilinear pairings [J]. Computers and Electrical Engineering, 2011, 37(4): 444-450.