

基于 Krawtchouk 不变矩的复制-粘贴篡改盲检测算法

黄子龙, 张政保, 文家福, 刘会英

(军械工程学院 计算机工程系, 河北 石家庄 050003)

摘要:针对数字图像检测中一类常见的复制-粘贴图像篡改, 提出一种基于小波变换和径向 Krawtchouk 不变矩的盲检测算法。算法利用小波变换提取图像的低频分量, 对低频分量分块提取径向 Krawtchouk 不变矩特征, 这种特征描述方式对图像旋转后处理具有鲁棒性, 然后将特征向量进行按字典排序, 并结合数学形态学进行图像复制篡改区域的检测和定位。实验表明该算法能有效地定位出复制和粘贴的图像篡改区域, 并对粘贴区域旋转操作具有很强的鲁棒性。

关键词: Krawtchouk 矩; 篡改检测; 盲检测; 旋转不变性

中图分类号: TN918

文献标识码: A

文章编号: 1673-629X(2012)02-0168-04

A Blind Forensic Algorithm for Detecting Copy-Paste Images Based on Krawtchouk Invariant Moments

HUANG Zi-long, ZHANG Zheng-bao, WEN Jia-fu, LIU Hui-ying

(Dept. of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: For a common class of copy-paste tampering in digital image forensics, a forensics algorithm is proposed based on Discrete Wavelet Transform (DWT) and radial krawtchouk invariance moment. The algorithm uses DWT to extract low frequency components of the image to propose the krawtchouk invariance moment of the blocks of low frequency of components. This characterization method is robust against image rotation. The feature vectors are then sorted according to the dictionary. Combined with mathematical morphology for image temper detection and region localization. Experiments show that the algorithm can locate the tampered region and strong robustness to the rotation of the paste region.

Key words: Krawtchouk moment; forgery detection; blind forensic; rotational invariance

0 引言

目前, 图像编辑软件以其使用简便、效果良好等特点广泛应用于图像处理领域。因此, 数字图像极易遭到篡改而不留下明显痕迹, 当这些被篡改的图片广泛应用于新闻报道以及司法取证等方面, 若这些篡改图片被轻易采用, 则易造成诈骗、虚假报道等极坏后果, 且易对民众造成财产损失。因此, 图像认证技术研究显得极为迫切和重要。

当前, 针对图像认证主要有主动认证和被动认证两种方式。主动认证方法除了基于数字签名的图像认证方法外, 主要还是采用基于脆弱数字水印^[1]的图像

认证方法。数字签名方法需冗余产生辅助信息, 并且签名内容容易遭到抛弃; 而脆弱水印方法需要对图像中嵌入水印信息, 对图像的质量和感知性易造成影响。基于这两种方法的弊端, 被动认证方法受到了广泛关注。数字图像被动认证也称为盲取证, 指在不依赖任何预签名提取或预嵌入信息的前提下, 对图像的真伪和来源进行鉴别。因此, 数字图像被动盲检测技术^[2,3]应运而生。其中一种重要的检测方式就是针对复制-粘贴篡改攻击进行检测的^[4-6]。

1 区域复制-粘贴篡改模型

区域复制粘贴^[7-10]是一种图像的局部篡改技术, 它把图像中的某一区域进行复制后, 粘贴到同一幅图像的不相交区域上, 以达到去除图像中某一重要目标或证据的目的。文中提出的算法以此作为判断图像是否被篡改的依据。由此得到区域复制-粘贴篡改模型为:

收稿日期: 2011-07-12; 修回日期: 2011-10-20

基金项目: 国家自然科学基金项目 (60772082); 河北省科技基金项目 (05213579)

作者简介: 黄子龙 (1986-), 男, 辽宁锦州人, 硕士研究生, 主要研究领域为信息安全; 张政保, 教授, 硕士生导师, 主要研究领域为信息安全。

(1) 复制区域和粘贴区域分别设为 D_1 和 D_2 , 其各自内部联通;

(2) 复制-粘贴区域可以不止一处, 多处可设为 $D_i, i = 1, 2, 3, \dots$ 。

(3) 被复制块与被粘贴块之间无交集, 即 $D_i \cap D_j = \emptyset, i \neq j$, 且 $i, j = 1, 2, 3, \dots$ 。

(4) 将复制区域和粘贴区域定量表示为其像素点间的位移为 $d = (\Delta x, \Delta y)$, d 的值应该大于某固定值 L 。

(5) 被复制区域应该是“较大面积区域”, 对于“较大面积区域”一般设定为原图面积的 0.85% 以上。

基于以上的假设条件, 可将复制-粘贴图像描述如下:

在一幅篡改图像 $f' = (D)$ 中, 必然存在两个区域 $D_1, D_i, i = 2, 3, \dots$, 及一个转移向量 $d = (\Delta x, \Delta y)$, ($|D_1| = |D_i| > |D| \times 0.85\%, |d| > L$)

s. t. $\forall (x_1, y_1) \in D_1, f' = (x_1, y_1) = f(x_2, y_2)$,
 $x_2 = x_1 + \Delta x, y_2 = y_1 + \Delta y, (x_2, y_2) \in D_i$

其中, $f(x, y)$ 是原始图像的灰度值, $D = \{(x, y) | 1 \leq x \leq M, 1 \leq y \leq N\}$, D_i 是被复制的区域, D_1 是被篡改的区域。因此, 篡改后的图像 f' 可表示为

$$f'(x, y) = \begin{cases} f(x, y), & (x, y \notin D_1) \\ f(x + \Delta x, y + \Delta y), & (x, y \in D_1) \end{cases} \quad (1)$$

本类型篡改检测主要是判别待检测图像中是否存在相似区域并确定其具体位置。在小波变换基础上基于块匹配的检测算法关键解决的问题是进行特征提取以及时间复杂度的迅速降低。

2 检测算法

2.1 小波变换

基于块匹配的检测算法需要解决的关键问题是时间复杂度和如何进行特征提取。本算法首先对待检测图像进行离散小波变换 DWT (Discrete Wavelet Transform)。小波变换是一种时域-频域 (或空域-频域) 变换, 同时具有时 (空) 域和频域的良好局部化性质。算法只对小波算法只提取小波的低频部分的特征, 其目的首先是减少图像块数, 且保证特征的鲁棒性, 因为低频部分对噪声并不敏感。

2.2 Krawtchouk 矩特征选取

● Krawtchouk 矩:

Krawtchouk 矩是基于经典的离散 Krawtchouk 多项式提出的一组新的正交矩。利用图像的 Krawtchouk 矩可以很好地恢复出原始图像。而且, 在不管有无噪声干扰的情况下都要比 Zernike、Legendre、Tchebichef 等矩性能更好。因为 Zernike 矩和 Legendre 矩是在连

续域上定义的正交矩, 在离散域中势必存在离散化误差, 且矩值动态范围较大。Tchebichef 矩和 Krawtchouk 矩在离散域具有正交性, 避免了上述问题。此外, 与 Tchebichef 矩相比, Krawtchouk 矩还具有从任何感兴趣图像区域中提取局部特征的优点。在 Krawtchouk 矩基础上, 本算法选取图像低频分量的径向 Krawtchouk 矩作为图像块特征, 结合检测算法, 对篡改图像的复制-粘贴区域进行检测和定位。

对于一幅数字图像 $f(x, y)$ 来说, 它的 Krawtchouk 矩被定义为^[11]:

$$Q_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \bar{K}_n(x; p_1, N-1) \bar{K}_m(y; p_2, M-1) f(x, y) \quad (2)$$

用于图像重建的逆变换定义为:

$$f(x, y) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} Q_{nm} \bar{K}_n(x; p_1, N-1) \times \bar{K}_m(y; p_2, M-1) \quad (3)$$

● Krawtchouk 径向矩^[12]:

径向矩用极坐标系统 (r, θ) 来表示。一幅图 $f(r, \theta)$ 在极坐标下的矩是由直角坐标用自变量为 θ 的函数来表示的。因为在一幅图片中 v 是圆周上最大像素数, θ 的变化范围在 $[0, 2\pi]$ 之间, $\theta_c = \frac{2\pi c}{v}, c = 0, 1, 2, \dots, v-1$ 。因此, 极坐标下径向 Krawtchouk 矩定义为:

$$R_{nm} = \frac{1}{v} \sum_{r=0}^{u-1} \sum_{c=0}^{v-1} \bar{K}_n(x; p_1, N-1) e^{-j\frac{2\pi cm}{v}} f(r, \theta_c) \quad (4)$$

其中 v 是当 r 取 $u-1$ 时, θ 从 0 到 2π 所取的步数, 对应于重建的逆变换为:

$$f(r, \theta_c) = \sum_{n=0}^{n_m} \sum_{m=0}^{m_m} R_{nm} \bar{K}_n(r; p, N-1) e^{+j\frac{2\pi cm}{v}} \quad (5)$$

径向矩定义在极坐标系统 (r, θ) 下笛卡尔坐标映射到极坐标下的对应关系为:

$$x = \frac{rN}{2(u-1)} \cos\left(\frac{2\pi c}{v}\right) + \frac{N}{2} \quad (6)$$

$$y = \frac{rN}{2(u-1)} \sin\left(\frac{2\pi c}{v}\right) + \frac{N}{2} \quad (7)$$

$$r = 0, 1, \dots, u-1, \theta = 0, 1, \dots, n.$$

最后得到径向 Krawtchouk 不变矩如下:

$$\varphi_n = R_{n0}$$

$$\varphi_{nm} = |R_{nm}|^2 \quad \text{for } m > 0$$

文中选用 $\varphi_1, \varphi_2, \varphi_{11}, \varphi_{21}$ 四个径向 Krawtchouk 不变矩来作为图像块特征, 其中取 $p = 0.5, u = N/2, v = 4N$ 。在实验过程中, 选取 512×512 的 tank 图像中以坐标 (117, 117) 为中心、半径为 5 的区域, 将其分别进行旋转 90° 、求取镜像块、添加高斯噪声等操作。首先计算原始块, 重叠相邻块 (117, 118), 进行处理操作后的所有块的径向 Krawtchouk 不变矩, 如表 1 所示。

表 1 图像的径向 Krawtchouk 不变矩

不变矩	原始块	相邻块	添加噪声块	旋转块	镜像块
φ_1	1.5664	1.8380	1.5673	1.5666	1.5668
φ_2	0.5934	0.8076	0.5936	0.5937	0.5934
φ_{11}	0.0081	0.0192	0.0087	0.0082	0.0081
φ_{21}	0.0242	0.0559	0.0256	0.0249	0.0248

实验表明,文中所选取的径向 Krawtchouk 不变矩对于噪声、图像几何形变等后处理具有一定的鲁棒性;同时与相邻块的差别较大,在进行算法匹配过程中性能良好。

2.3 算法描述

2.3.1 阈值选择

(1) 图像块相似阈值。将图像块相似阈值设为 R , 提取图像块的特征向量并且比较它们的相似性是块匹配复制-粘贴检测算法的核心。将特征向量进行排序后, 即可在每个 V_j 相邻的空间范围之内, 来寻求符合相似判决条件的图像块。为了衡量特征向量 V_i 和 V_j 之间的相似度, 定义:

$$R = \sqrt{(V_i - V_j) \otimes (V_i - V_j)} \quad (8)$$

上式中, \otimes 表示内积。通过实验, 随机选取篡改块大小为 18×18 的篡改图像 200 幅, 并对这些篡改图像进行后处理操作, 如高斯模糊和高斯白噪声等。在经过篡改后的图像中, 对比篡改块所在区域和原始块所在区域之间的变化, 并将其平均值设为 R 的值。

(2) 图像移动向量的阈值。将该阈值设为 L , 在块相似匹配的过程当中, 若块之间有重叠区域, 则会由于其相似度的增高, 造成虚警率较高, 基于以上原因, 提出了移动向量的阈值。将块的大小设为 $b \times b$, 移动向量阈值 $L > \sqrt{b \times b + b \times b}$ 。

(3) 区域面积阈值 S 。通过大量的统计实验, 得出结论: 若检测到在一幅图像中存在大面积的相似区域, 则很有可能是被区域复制篡改过的。进行图像检测时, 图像检测到的块与原始图像块之间往往会存在一定的差别, 原因是图像可能是受到了位置的后处理操作。 $S > 512 \times 512 \times 0.85\%$ 。

(4) 对于初步检测到的结果需要利用数学形态学的方法进行相应处理, 其目的主要通过填补联通区域内存在的一些“空洞”, 这样可得到较好的检测结果。

2.3.2 算法步骤

设待检测的图像为 $I_{M \times N}$, 其大小为 $M \times N$ 。

Step1: 对待检测图像进行 j 级小波变换, 待检测的低频子带大小为 $M \times N$, 分块后的小波低频图像为 $A_{m \times n}$, 其中 $m = \lceil M/2^j \rceil$, $n = \lceil N/2^j \rceil$;

Step2: 将 $A_{m \times n}$ 分解为有重叠区域的 $b \times b$ 的小块, 一共得到 $\text{Sum} = (m - b + 1) \times (n - b + 1)$ 个图像块;

Step3: 对每个分块提取径向 Krawtchouk 不变矩作为特征向量 $V_j, j = 1, 2, 3, \dots, \text{Sum}$, 每个 V_j 作为一个

列向量存储在 Krawtchouk 特征向量矩阵的第 j 列;

Step4: 将所有的向量 $V_j, j = 1, 2, 3, \dots, \text{Sum}$ 按照相似度的值进行字典排序, 得到排序后特征向量矩阵;

Step5: 通过阈值判断和数学形态学定位, 最终定位出篡改区域。

3 实验结果及分析

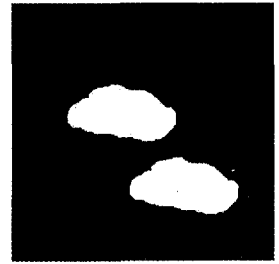
为了验证文中提出的图像复制-粘贴盲检测算法的有效性, 选取大小为 512×512 的 256 级灰度图像 (RGB 图像可以转化为灰度图像) 对算法进行了实验验证。经过随机选择 200 幅图像做区域复制篡改, 对篡改图像做不同的后处理操作 (高斯白噪声、高斯模糊等), 比较原始块所在区域与篡改块所在区域之间的变化, 利用公式 (8), 求其平均值, 相似度阈值 $R = 0.5$; 匹配块半径设为 5, 则移动向量阈值 $L = 10$; 定义区域面积阈值 $S > 512 \times 512 \times 0.85\%$ 。在实验过程中, 选取的灰度图如图 1(a), 图 1(b) 即经过图 1(a) 篡改后得到的, 在不经其他处理时, 检测结果如图 1(c) 所示。



(a) 原始图像



(b) 篡改图像



(c) 检测结果

图 1 原始检测结果

算法的鲁棒性是文中研究的重点之一, 为验证这一点, 首先通过不同操作处理图像, 如添加高斯噪声等得到检测结果分别如图 2 所示。

通过实验结果可知, 添加了不同的高斯噪声后, 算法能够较好地抵抗高频信号的干扰, 主要原因是算法中提取的特征来自图像的低频子带, 且特征为具有一定鲁棒性的低阶几何不变矩, 具有一定的抗几何形变的特性。对篡改区域进行旋转和镜像操作, 篡改图像和检测结果如图 3 所示。

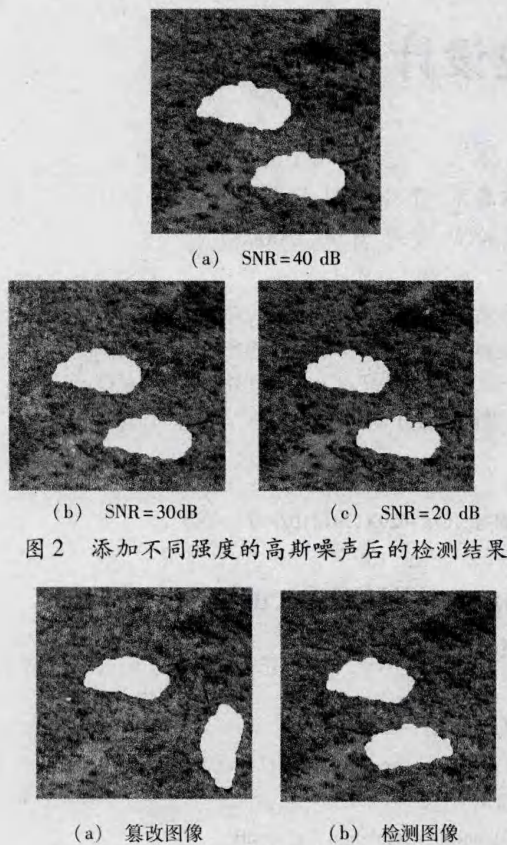


图 2 添加不同强度的高斯噪声后的检测结果

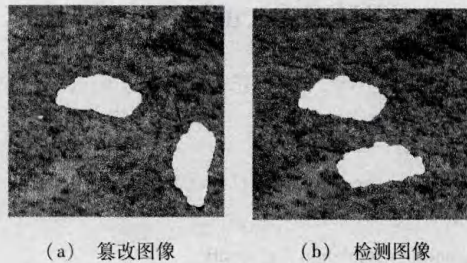


图 3 被粘贴区域镜像处理后的检测结果

由此可以看出,文中算法对经过镜像和篡改等相关操作的检测效果良好,为了研究算法的有效性和对加噪、旋转、镜像等操作的鲁棒性,随机选取 200 幅大小为 512×512×8 (bits) 的灰度图像进行篡改。在实验中,为了对图像篡改区域的定位结果进行定量分析,定义检测率 r 和错误率 w 为:

$$r = \frac{|D_1 \cap R_1| + |D_2 \cap R_2|}{|D_1| + |D_2|} \tag{9}$$

$$w = \frac{|D_1 \cup R_1| + |D_2 \cup R_2|}{|D_1| + |D_2|} - r \tag{10}$$

表 2 原始检测结果

篡改区域	正确率	错误率	误判率
32×32	0.9644	0.0677	0
64×64	0.9723	0.0519	0
96×96	0.9794	0.0405	0
128×128	0.9903	0.0172	0

从实验结果可以看出,本算法对篡改图像进行检测时,篡改区域越大,检测效果越明显,在篡改区域为 128×128 时,其篡改正确检测率高达 99.03%;同时,高频信号的加入与检测的准确性呈负相关关系,即信号强度越小,则算法检测准确率越高。通过实验可知,文中算法能够有效地检测复制-粘贴篡改图像并定位篡改区域,而且对篡改后的图像处理具有较强的鲁棒性,通过对大量图片检测其抗旋转攻击性能,其结果如表

2.3 所示,达到良好效果。

表 3 添加不同强度的高斯噪声后的误判率

噪声参数	篡改区域			
	32×32	64×64	96×96	128×128
20	0.105	0.075	0.05	0.035
25	0.075	0.05	0.02	0.015
30	0.05	0.025	0.01	0.015
35	0.01	0.015	0.005	0.005
40	0.01	0.01	0	0

4 结束语

针对常见的复制-粘贴篡改攻击,文中提出一种有效的检测与定位篡改区域算法,该算法通过小波分解,减少块总数,降低时间复杂度,同时提取图像块的 Krawtchouk 不变矩,由于径向 Krawtchouk 矩本身具有旋转不变性,因此,应用在图像复制-粘贴篡改的检测中效果明显。

参考文献:

[1] 吴金海,林福宗.基于数字水印的图像认证技术[J].计算机学报,2004,27(9):1153-1161.

[2] 吴琼,李国辉,涂丹,等.面向真实性鉴别的数字图像盲取证技术综述[J].自动化学报,2008,34(12):1458-1466.

[3] 魏为民,王朔中,唐振军,等.一类数字图像篡改的被动认证[J].东南大学学报,2007,37(A01):58-61.

[4] 王鑫,鲁志波.数字图像拷贝移动篡改检测方法的分析[J].计算机工程与设计,2009,30(12):2989-2991.

[5] 王俊文,刘光杰,张洪,等.图像区域复制篡改快速鲁棒取证[J].自动化学报,2009,35(12):1487-1495.

[6] Luo W Q, Qu Z H, Pan F, et al. A survey of passive technology for digital image forensics[J]. Front Comput Sci China, 2007, 1(2):166-179.

[7] Biehl I, Meyer B, Mller V. Differential Fault Attacks on Elliptic Curve Cryptosystems[C]//CRYPTO'00, LNCS. [s. l.]: Springer-Verlag, 2000:131-146.

[8] 骆伟祺,黄继武,丘国平.鲁棒的区域复制图像篡改检测技术[J].计算机学报,2007,30(11):1998-2007.

[9] Ng T T, Chang S F, Lin C Y, et al. Passive-blind image forensics in multimedia security technologies for digital rights[M]. Orlando: Academic Press, 2006:383-412.

[10] Mahdian B, Saie S. Detection of copy-move forgery using a method based on blur moment invariants[J]. Forensic Science International, 2007, 171:180-189.

[11] Yap P T, Paramesran R, Ong S H. Image Analysis by Krawtchouk Moments[J]. IEEE Transactions on Image Processing, 2003, 12(11):1367-1377.

[12] Raj P A, Venkataramana A. Radial Krawtchouk Moment for Rotational Invariant Pattern Recognition[C]//ICICS07. [s. l.]: [s. n.], 2007.