计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190600081

基于 DCT 系数哈希的图像篡改检测算法

尚进跃　毕秀丽　肖　斌　李伟生
重庆邮电大学计算智能重点实验室　重庆 400065
(864143390@qq.com)

摘　要　随着数字图像处理技术的不断提高,大量的篡改图像充斥互联网和各类媒体,严重影响了人们的日常生活。因此,对图像的真实性和完整性进行判断的数字图像取证技术显得尤其重要。针对数字图像版权中常见的剪切组合篡改问题,文中提出了一种基于 DCT 系数哈希的图像篡改检测算法。在 JPEG 压缩过程中,首先提取 Y 通道的 DCT 系数矩阵,然后对所提系数矩阵进行 DCT 以构造出图像哈希,最后将图像哈希嵌入压缩码流的文件头。在篡改检测时,通过篡改图像对应的压缩码流构造出篡改图像哈希,将其与嵌入的源图像哈希进行比较以进行初次检测。为了达到像素级检测的目的,文中在初次检测结果的基础上提出了一种二次检测的算法。实验结果表明,所提算法不仅鲁棒性较好,而且构造的图像哈希长度较短,检测的准确率也提高了 10%。

关键词:图像哈希;JPEG 压缩;2D-DCT;图像篡改检测
中图法分类号　TP301

Image Forgery Detection Based on DCT Coefficients Hashing

SHANG Jin-yue,BI Xiu-li,XIAO Bin and LI Wei-sheng
Chongqing Key Laboratory of Computational Intelligence,Chongqing University of Posts and Telecommunications,Chongqing 400065,China

Abstract　With the continuous improvement of digital image processing technology,tampered images are flooded with the Internet and various media,seriously affecting people's daily life. Therefore,digital image forensics technology,which can judge the authenticity and integrity of images,is particularly important. An image forgery detection algorithm based on DCT coefficients hashing was proposed,for dealing with the splicing forgery detection of digital images. In the process of JPEG compression,first,the DCT coefficient matrix of the Y channel after DCT is extracted,then the image hashing is constructed by DCT coefficients,and finally the image hashing is embedded in the header of file of the compressed code stream. At the time of tampering detection,a tampering image hashing is constructed by compressed code stream corresponding to the tampering image,and then compared with the embedded original image hashing for initial detection. In order to achieve the pixel-level detection,a method of secondary detection was proposed based on the preliminary detection results. The experimental results show that the proposed algorithm not only has good robustness,but also has a shorter hash length and a 10% higher detection accuracy.

Keywords　Image hashing,JPEG compression,2D-DCT,Image forgery detection

1　引言

随着科技的进步和发展,各种图像编辑软件日益普及,致使数字图像的恶意篡改现象越来越多[1]。颜色变化、复制移动伪造、剪切组合及克隆等是目前一些流行的图像篡改操作。图 1 给出了一个图像拼接篡改的示例。

(a)源图像　(b)篡改图像　(c)真实篡改区域

图 1　剪切组合篡改示例

Fig. 1　Example of splicing

篡改图像充斥互联网和各类媒体,严重影响了人们的日常生活,而且如果篡改图像被用于官方媒体、科学发现及法庭证物等,无疑将会对政治和社会稳定产生严重的影响。因此,篡改检测作为一种识别数字多媒体数据完整性和原始性的方案,已成为一个重要的研究领域。

近年来,基于图像哈希的篡改检测方法得到了广泛的研究。图像哈希是一种用一个紧凑签名来表示图像视觉内容的技术,其所构造的哈希必须对常见的图像攻击具有鲁棒性,但对恶意操作敏感。Venkatesan 等[2]首先引入了图像哈希的概念,他们使用小波系数的非可逆压缩作为描述符来生成哈希,考虑了压缩、几何失真和一些其他攻击的鲁棒性。Monga 等[3]提出了一种图像认证框架,利用显著特征点和 Hausdorff 距离生成图像哈希,该算法对大多数标准的基准测试攻击具有较强的鲁棒性,但认证精度不高。

为了实现篡改定位的目的,Roy 等[4]第一次提出使用图

到稿日期:2019-06-14　返修日期:2019-08-13　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:毕秀丽(bixl@cqupt.edu.cn)

像哈希来进行篡改检测。该方法将图像的边缘分割成大小为 16×16 不重叠块，以查找图像中的篡改区域，对旋转、剪切和压缩具有一定的鲁棒性。Ahmed 等[5]将图像分割为 16×16 块，进行小波变换来寻找篡改内容，但是这种方法只能对图像压缩、高通滤波及低通滤波具有鲁棒性。为了在几何变换情况下也能准确检测篡改区域，一些学者提出了图像对齐技术。Lu 等[6]将 SIFT 特征编码成紧凑视觉单词(Compact Visual Word)来估计几何变换，然后通过 SIFT 和基于块的边缘方向统计图来来检测和定位篡改区域。Battiato 等[7]利用方向导数的统计图来实现图像块级别的篡改检测和定位。

随后，一些研究学者又提出基于图像分割构建图像哈希的方法，此类方法的检测结果优于之前的方法。Lv 等[8]先将图像分割成不同的环形和扇形，然后使用 SIFT-Harris 检测子构造图像哈希值，通过这种方法生成的图像哈希对大范围的几何攻击都有很好的鲁棒性，但是，由于检测方法使用 Random 变换来估计篡改区域的中心方向，因此当篡改区域在图像中间位置时，检测会失败。Zhao 等[9]利用 Zernike 矩和图像局部特征来设计图像哈希，该方法只能检测到篡改区域明显的情况，并且对于各种攻击的鲁棒性不强。Wang 等[10]将基于图像块和基于特征点的方法相结合来构造图像哈希，这种方法虽然能实现篡改区域的准确定位，但是图像哈希长度达到万级，需要占用较大的存储空间。Yan 等[11]将图像分割成环形和扇形以构建多尺度图像哈希来检测篡改区域。Tang 等[12]利用图像的环形分割和向量不变距离来提升图像哈希的鲁棒性和识别能力，但是该方法无法实现篡改区域的准确定位。Pun 等[13]将图像自适应地进行分割，然后利用图像哈希实现目标类篡改的检测，但是如果篡改区域具有平滑纹理，则分割算法无法切分出篡改区域，该方法就会失效。Yan 等[14]使用四元数傅里叶梅林变换和四元数傅里叶变换构造图像哈希，该方法可以检测图像颜色变化、复制粘贴和剪切组合篡改，但是全局特征没有办法实现小尺度篡改区域和多个不联系篡改区域的检测。Yan 等[15]提出了二值排序哈希方法，并通过多尺度分析得到最终的定位结果。

针对以上篡改检测算法存在的哈希长度较长和检测准确率较低的问题，本文提出了一种基于 DCT 系数哈希的图像篡改检测算法。在 JPEG 压缩过程中，首先提取 Y 通道的 DCT 系数矩阵，然后对提取的系数矩阵进行离散余弦变换 DCT 从而构造出图像哈希，最后将图像哈希嵌入压缩码流的文件头。在篡改检测时，首先通过篡改图像对应的压缩码流构造出篡改图像哈希，然后将其与嵌入的源图像哈希进行比较以完成初次检测。基于块的检测方法会导致检测结果出现块现象，为解决此问题，本文在初次检测结果的基础上提出了一种二次检测算法，通过该算法最终可以得到像素级的检测结果。

本文第 2 节介绍基于 DCT 系数的图像哈希的构造方法；第 3 节详细介绍篡改检测流程；第 4 节验证所提算法在检测结果准确性和鲁棒性等方面的优势；最后总结全文。

2 基于 DCT 系数的图像哈希

JPEG 是目前一直使用的应用最广的图像压缩标准，它以有损压缩的方式去除冗余的图像数据，在获得极高的压缩率的同时能展现十分丰富生动的图像，目前大部分图像都是以 JPEG 格式进行保存。JPEG 压缩的具体流程分为颜色空间转换、分块、DCT、量化和编码，然后得到最终的压缩数据码流。本文将 JPEG 压缩和图像哈希的构造过程相结合，实现了在对图像进行 JPEG 压缩的过程中便可以快速地完成图像哈希的构造和嵌入。

图像哈希是一种生成一个独特签名并以紧凑的方式来表示图像视觉内容的方案，已被广泛用于图像检索[16-18]、篡改检测[8,19]和信息认证[20]等方面。用于篡改检测的图像哈希必须对常见的图像攻击具有鲁棒性，但对图像受到的恶意篡改操作敏感。本文所提出的图像哈希由两部分组成：基于 DCT-DC 系数的 DC 哈希 $\boldsymbol{H}_{DC}$ 和基于 DCT-AC 系数的 AC 哈希 H_{AC}。所提出的图像哈希的具体构造流程如图 2 所示。

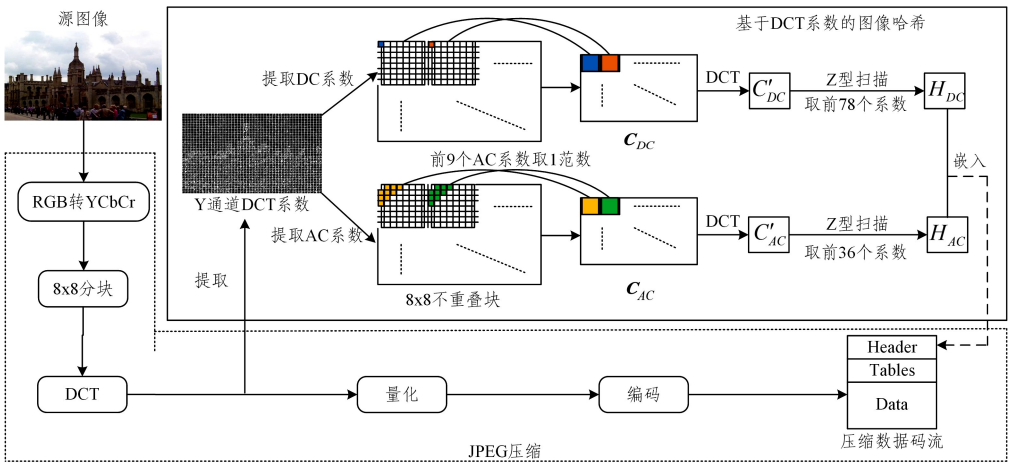


图 2 基于 DCT 系数的图像哈希的构造框架

Fig. 2 Construction framework of image hash based on DCT coefficients

在对图像进行 JPEG 压缩的过程中，通过提取 DCT 之后 Y 通道的 DCT 系数矩阵来完成 DC 哈希和 AC 哈希的构造：

(1)提取 Y 通道 DCT 系数矩阵的每个大小为 8×8 的块的 DC 系数，组成 DC 系数矩阵 $\boldsymbol{C}_{DC}$，对 $\boldsymbol{C}_{DC}$ 进行二维 DCT 得到 $\boldsymbol{C}_{DC}'$，按 Z 字型扫描 $\boldsymbol{C}_{DC}'$，取其前 78 个系数作为 DC 哈希 $\boldsymbol{H}_{DC}$；

(2)提取 Y 通道 DCT 系数矩阵的每个大小为 8×8 的块的前 9 个 AC 系数，计算所取系数的 1 范数，将该 1 范数记为

块 AC 系数，这样每个大小为 8×8 的块都对应于一个块 AC 系数。提取每个大小为 8×8 的块的块 AC 系数组成块 AC 系数矩阵 $\boldsymbol{C}_{AC}$，对 $\boldsymbol{C}_{AC}$ 进行二维 DCT 得到 $\boldsymbol{C}_{AC}'$，同样按 Z 字型扫描 $\boldsymbol{C}_{AC}'$，取其前 36 个系数作为 AC 哈希 $\boldsymbol{H}_{AC}$。

最后，将构造的图像哈希 $\boldsymbol{H}=[\boldsymbol{H}_{DC}\ \ \boldsymbol{H}_{AC}]$ 存储到通过 JPEG 压缩得到的压缩数据码流的文件头，后期在对图像进行篡改检测时可以将其提取出来使用。

3 图像篡改检测

图像篡改检测是对人为恶意修改而改变视觉信息的图像内容进行定位的过程。在传统的基于图像哈希的篡改检测算法中，对给定的一幅篡改图像进行篡改检测时，首先应从篡改图像文件中提取出之前存储的源图像的图像哈希，然后与构造出的篡改图像的图像哈希进行比较，以得出最终的篡改检测结果。

本文提出的篡改检测算法由两部分组成。

(1)首先从篡改图像对应的压缩数据码流的文件头中提取出之前存储的源图像的图像哈希 $\boldsymbol{H}^S$，然后通过篡改图像对应的压缩数据码流构造出篡改图像的图像哈希 $\boldsymbol{H}^R$，将 $\boldsymbol{H}^S$ 和 $\boldsymbol{H}^R$ 进行比较，得到初次的篡改检测结果。

(2)由于初次检测结果的准确度较低且存在块效应，因此本文提出在初次检测结果的基础上，利用 DC 哈希 H_{DC}^S 和篡改图像的 Y 通道进行二次检测，进而得到准确度更高的像素级检测结果。

3.1 基于 DC 哈希和 AC 哈希的初次篡改检测

图 3 给出了基于 DC 哈希和 AC 哈希的初次检测框架。对一幅大小为 $\boldsymbol{Z}=[\boldsymbol{M}_0\ \ \boldsymbol{N}_0]$ 的篡改图像 $f^R(x,y)$ 进行检测时，首先从 $f^R(x,y)$ 对应的压缩数据码流的文件头中提取出之前存储的源图像的图像哈希 $\boldsymbol{H}^S$：

$$\boldsymbol{H}^S=[\boldsymbol{H}_{DC}^S\ \ \boldsymbol{H}_{AC}^S] \tag{1}$$

然后，根据第 2 节提出的图像哈希构造方法，利用篡改图像对应的压缩数据码流构造出篡改图像 $f^R(x,y)$ 的图像哈希 $\boldsymbol{H}^R$：

$$\boldsymbol{H}^R=[\boldsymbol{H}_{DC}^R\ \ \boldsymbol{H}_{AC}^R] \tag{2}$$

最后，对哈希 $\boldsymbol{H}_{DC}^S$，$\boldsymbol{H}_{DC}^R$，$\boldsymbol{H}_{AC}^S$ 和 $\boldsymbol{H}_{AC}^R$ 分别进行二维余弦反变换，将变换得到的结果分别用 $\boldsymbol{f}_{DC}^S$，$\boldsymbol{f}_{DC}^R$，$\boldsymbol{f}_{AC}^S$ 和 $\boldsymbol{f}_{AC}^R$ 表示，然后分别计算差值：

$$\boldsymbol{D}_{DC}=|\boldsymbol{f}_{DC}^S-\boldsymbol{f}_{DC}^R| \tag{3}$$

$$\boldsymbol{D}_{AC}=|\boldsymbol{f}_{AC}^S-\boldsymbol{f}_{AC}^R| \tag{4}$$

其中，$|\cdot|$ 表示取绝对值。

为获得篡改检测结果，需将 $\boldsymbol{D}_{DC}$ 和 $\boldsymbol{D}_{AC}$ 分割为篡改部分和非篡改部分，因此，考虑使用最大类间方差法(Otsu)作为本文中的阈值分割方法。

利用最大类间方差法对差值矩阵 $\boldsymbol{D}_{DC}$ 和 $\boldsymbol{D}_{AC}$ 进行阈值分割，得到分割后对应的二值图 $\boldsymbol{B}_{DC}$ 和 $\boldsymbol{B}_{AC}$；然后，对二值图 $\boldsymbol{B}_{DC}$ 和 $\boldsymbol{B}_{AC}$ 进行形态学闭操作，得到处理后的结果 $\boldsymbol{B}_{DC}'$ 和 $\boldsymbol{B}_{AC}'$；最后，对 $\boldsymbol{B}_{DC}'$ 和 $\boldsymbol{B}_{AC}'$ 进行与操作，得到初次的检测结果 $\boldsymbol{B}_1$：

$$\boldsymbol{B}_1=\boldsymbol{B}_{DC}'\times\boldsymbol{B}_{AC}' \tag{5}$$

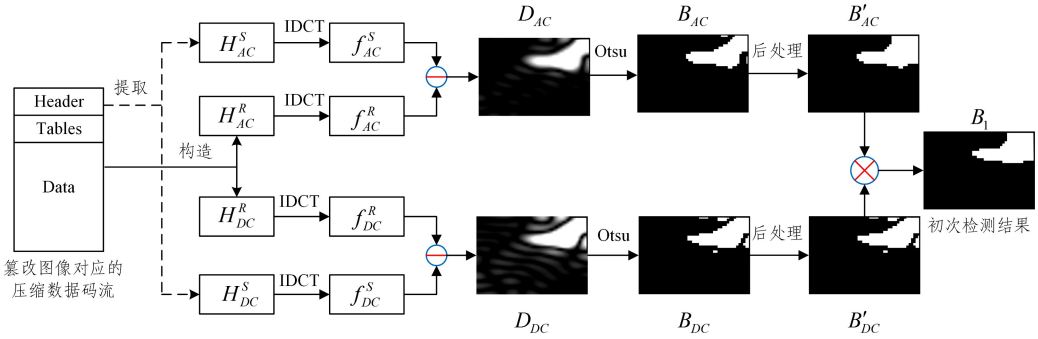


图 3 基于 DC 哈希和 AC 哈希的初次检测框架

Fig. 3 Initial detection framework based on DC hash and AC hash

3.2 基于篡改图像、DC 哈希和初次检测结果的二次篡改检测

通过初次篡改检测得到的检测结果准确度较低且具有块效应，因此本文在初次检测结果的基础上利用 DC 哈希 $\boldsymbol{H}_{DC}^S$ 和篡改图像的 Y 通道进行二次检测，从而获得准确度更高的像素级篡改检测结果。二次检测的具体流程如图 4 所示。

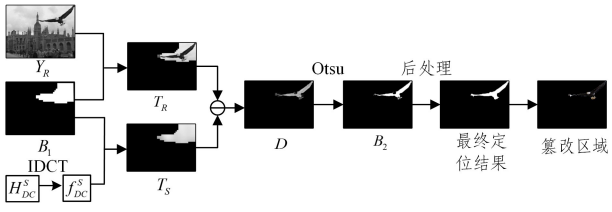


图 4 二次检测框架

Fig. 4 Framework of secondary detection

为了表示方便，用 $P=\{P_1,P_2,\cdots,P_N\}$ 表示 $f^R(x,y)$ 的 N 个大小为 8×8 的不重叠块。首先，提取篡改图像 $f^R(x,y)$ 的 Y 通道，记为 $\boldsymbol{Y}_R$，对 $\boldsymbol{Y}_R$ 进行如下操作：

$$\boldsymbol{Y}_R(P_i)=\{\boldsymbol{Y}_R(P_i)=0,\text{if } \boldsymbol{B}_1(i)=0\}_{i=1}^N \tag{6}$$

其中，$\boldsymbol{Y}_R(P_i)$ 表示 $\boldsymbol{Y}_R$ 的第 i 个大小为 8×8 的块，$\boldsymbol{B}_1(i)$ 表示初次检测结果 $\boldsymbol{B}_1$ 的第 i 个系数，将 $\boldsymbol{Y}_R$ 经式(6)计算后的结果记为 $\boldsymbol{T}_R$。

定义一个大小为 $\boldsymbol{Z}=[\boldsymbol{M}_0\ \ \boldsymbol{N}_0]$ 的零矩阵 $\boldsymbol{I}_0$。若 $\boldsymbol{B}_1(i)=1$，则把 $\boldsymbol{f}_{DC}^S(i)$ 赋给 $\boldsymbol{I}_0(P_i)$ 的第一个系数，其中，$i=1,2,\cdots,N$，$\boldsymbol{f}_{DC}^S$ 由 $\boldsymbol{H}_{DC}^S$ 二维余弦反变换得到，$\boldsymbol{I}_0(P_i)$ 表示 $\boldsymbol{I}_0$ 的第 i 个大小为 8×8 的块，$\boldsymbol{f}_{DC}^S(i)$ 表示 $\boldsymbol{f}_{DC}^S$ 的第 i 个系数。

然后，对 $\boldsymbol{I}_0$ 的每个大小为 8×8 的块进行二维余弦反变换得到 $\boldsymbol{T}_S$。通过计算 $\boldsymbol{T}_R$ 和 $\boldsymbol{T}_S$ 之间的差值并取绝对值，得到差值矩阵 $\boldsymbol{D}$：

$$\boldsymbol{D}=|\boldsymbol{T}_R-\boldsymbol{T}_S| \tag{7}$$

同样，利用最大类间方差法对计算得到的差值矩阵 $\boldsymbol{D}$ 进行阈值分割，把分割后的二值图结果记为 $\boldsymbol{B}_2$，对 $\boldsymbol{B}_2$ 进行形态

学闭操作，即可得到最终的定位结果。

4 实验结果与分析

4.1 实验数据集的选择

本文利用篡改图像数据集 CASIA v2.0 对所提算法进行评价。数据集 CASIA v2.0 由 1175 组剪切组合篡改图像数据组成，图像大小的范围为 240×160 至 900×600，图像内容包括风景、动物、建筑、人物、植物及物品等，丰富的图像内容可以对所提算法的有效性进行更全面的评价。

4.2 评价指标

本文利用 3 个评价指标（精确度 precision、召回率 recall 和 F-measure）对所提算法的篡改定位效果进行评价。精确度 precision 指正确分配给检测区域的像素数相对于篡改像素数的百分比；而召回率 recall 指正确分配给检测区域的像素数相对于真实篡改像素数的百分比；F-measure 则是整体性能的度量，如果 F-measure 的值越大，检测算法的检测效果就越好。F-measure 由 precision 和 recall 计算得到：

$$F\text{-}measure=\frac{2}{1/precision+1/recall} \tag{8}$$

4.3 哈希长度的选择

本文算法中，用来构造 DC 哈希和 AC 哈希的系数个数至关重要，它既决定了最终篡改定位结果的好坏，又决定了哈希的长度。为了确定构造 DC 哈希和 AC 哈希的系数个数，本文对 1175 组篡改图像进行了测试。表 1 列出了当 DC 哈希和 AC 哈希取不同系数个数时对应的 F-measure 平均值。由表 1 可知，组成 DC 哈希和 AC 哈希的系数个数越少，哈希长度就越短，但最终篡改定位的准确性较低；组成 DC 哈希和 AC 哈希的系数个数越多，最终的定位准确性就越高，但哈希长度较长。综合考虑哈希长度和最终的篡改定位准确度，本文取组成 DC 哈希的系数个数为 78，取组成 AC 哈希的系数个数为 36，按每个系数占 8 bits 来计算，则本文所构造的最终图像哈希长度为 912 bits。

表 1 DC 哈希和 AC 哈希取不同系数个数时的 F-measure

Table 1 F-measure when DC hash and AC hash take different coefficients

组成 DC 哈希的系数个数	组成 AC 哈希的系数个数					
	36	45	55	66	78	91
36	0.6041	0.6209	0.6401	0.6541	0.6668	0.6785
45	0.6243	0.6332	0.6495	0.6623	0.6744	0.6858
55	0.6416	0.6480	0.6588	0.6704	0.6818	0.6926
66	0.6586	0.6632	0.6713	0.6791	0.6888	0.6981
78	0.6719	0.6765	0.6824	0.6883	0.6956	0.7036
91	0.6858	0.6899	0.6951	0.6999	0.7058	0.7119

4.4 评价实验和对比分析

为了对所提算法的定位效果进行评价，本文选择 SCH[8]，QBH[14] 和 BRH[15] 算法作为对比算法。在对比过程中，SCH[8]，QBH[14] 和 BRH[15] 算法所用到的参数和相应论文中所用的参数一样。

本文从实验数据集中随机挑选 6 组作为示例，对不同算法的检测效果进行对比，如图 5 所示。

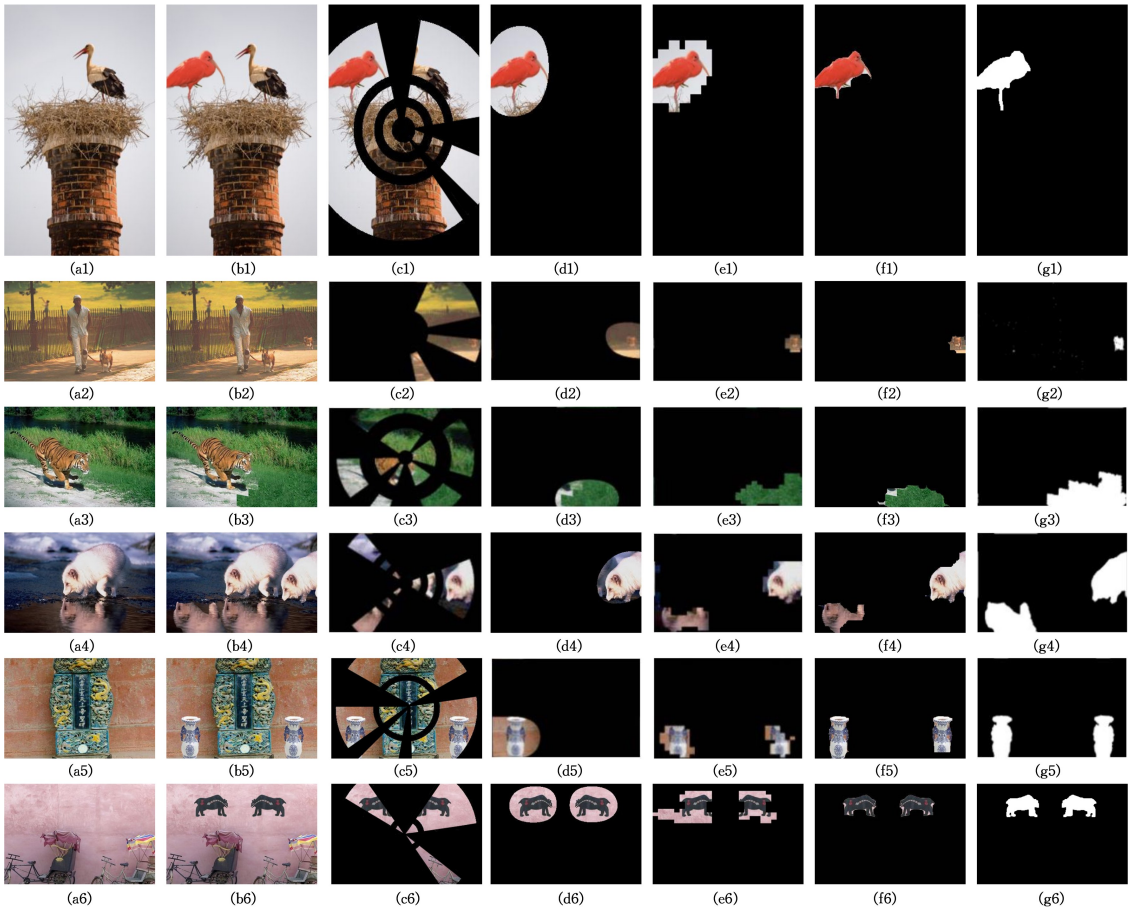


图 5 不同检测算法的检测结果对比

Fig. 5 Comparison of detection results of different detection algorithms

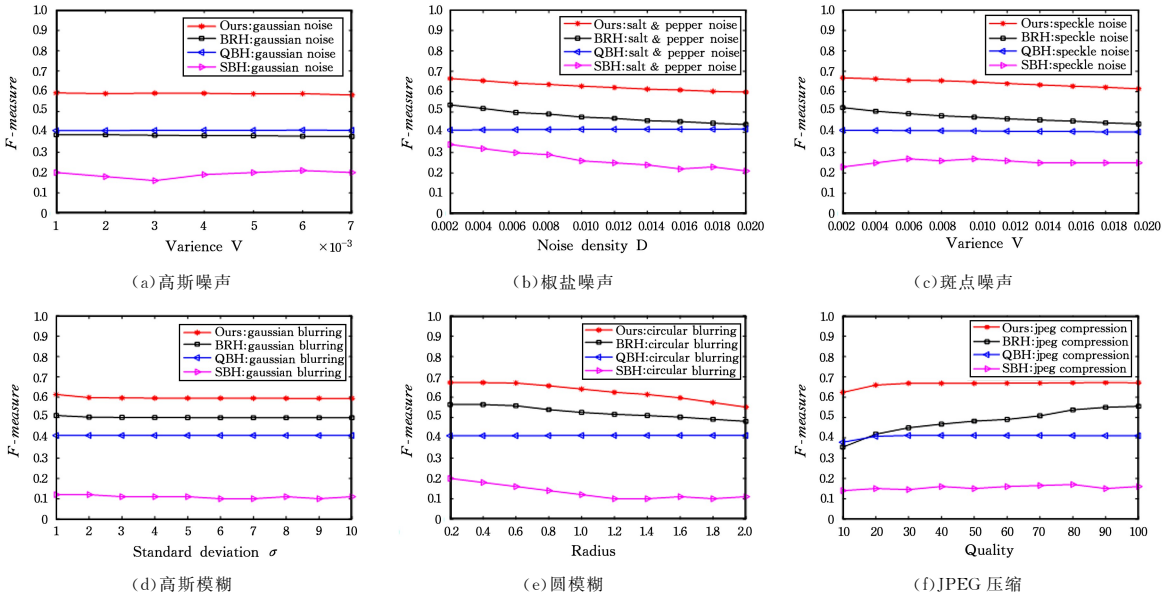
图 5 中，第 a 列表示源图像；第 b 列表示篡改图像；第 c 列表示 SCH[8] 的检测结果，第 d 列表示 QBH[14] 的检测结果；第 e 列表示 BRH[15] 的检测结果；第 f 列表示本文算法的检测结果；第 g 列表示真实篡改区域。从主观视角出发，可以发现 SCH[8] 的检测结果基本失效，QBH[14] 和 BRH[15] 虽然可以定位出篡改区域，但 QBH[14] 的检测结果的定位区域太大，准确率较低，算法 QBH[14] 的检测结果存在明显的块效应。而本文算法的检测结果优于其他 3 种算法，更加接近真实的篡改区域。

为了验证所提算法提升检测准确率的效果，本文将 SCH[8]，QBH[14] 和 BRH[15] 算法与本文算法在数据集上进行测试，并对 F-measure 平均值进行统计，统计结果如表 2 所列。由表 2 可知，本文算法的检测结果在准确率上高于其他 3 种算法，可以在检测时获得更好的检测效果。进一步地，为验证所提算法的鲁棒性，本文对篡改图像添加 6 种不同的图像攻击（高斯噪声、椒盐噪声、斑点噪声、高斯模糊、圆模糊以及 JPEG 压缩），并在不同图像攻击下，对 SCH[8]，QBH[14]，BRH[15] 和本文算法的 F-measure 平均值进行了统计，结果如图 6 所示（图 6(a)－图 6(f)分别为按顺序对应添加 6 种图像攻击）。由图 6 可知，本文算法在各种图像攻击下的 F-measure 平均值高于其他 3 种算法，并且整体 F-measure 平均值波动较小，由此可证本文算法可以抵抗常见的图像攻击。

表 2 不同检测算法的 *F-measure*

Table 2 *F-measure* of different detection algorithms

算法	*F-measure*
SCH[8]	0.1916
QBH[14]	0.4103
BRH[15]	0.5637
本文算法	0.6719



(a)高斯噪声 (b)椒盐噪声 (c)斑点噪声

(d)高斯模糊 (e)圆模糊 (f)JPEG 压缩

图 6 不同攻击下篡改检测结果的对比

Fig. 6 Comparison of tampering detection results under various attack

为了对所提算法的检测效果做出更全面的评价，本节将所提算法的时间复杂度和哈希长度与 SCH[8]，QBH[14] 和 BRH[15] 算法进行对比，结果如表 3 所列。

表 3 不同检测算法的时间复杂度和哈希长度

Table 3 Time complexity and hash length of different detection algorithms

算法	256×384 检测时间/s	600×800 检测时间/s	哈希长度/bits
SCH[8] 算法	8.4593	32.2561	480
QBH[14] 算法	2.6203	5.3990	1376
BRH[15] 算法	9.6469	39.1075	1200
本文算法	0.9236	4.5330	912

表 3 列出了 4 种算法在检测大小为 256×384 和 600×800 的篡改图像时所用的时间，并列出了 4 种算法所构造的图像哈希长度，由对比结果可知，所提算法的检测速度更快且哈希长度比 QBH[14] 和 BRH[15] 更短。虽然 SCH[8] 的哈希长度较本文算法更短，但由表 2 知 SCH[8] 的 F-measure 平均值很低，且由图 5 中的第 3 列可知 SCH[8] 算法的检测结果基本失效。因此，本文算法更具有优势。

结束语 本文提出了一个基于 DCT 系数的图像哈希，用于进行彩色图像的篡改检测，将 JPEG 压缩和图像哈希的构造过程相结合，实现了在对图像进行 JPEG 压缩的过程中便可快速完成图像哈希的构造和嵌入。为了达到像素级检测的目的，本文在初次检测结果的基础上还提出了一种二次检测算法。与代表性的基于图像哈希的篡改检测算法相比，所提算法构造的图像哈希的长度更短，且最终的检测准确率提高了 10%左右。在未来的工作中，可以考虑优化现有的后处理方法，以进一步提高篡改检测的准确度。

参 考 文 献

[1] MISHRA M. Digital Image Tamper Detection Techniques－A Comprehensive Study[J]. Computer Science, 2013, 2(1): 1-12.

[2] VENKATESAN R, KOON S M, JAKUBOWSKI M H, et al. Robust Image Hashing[C]// International Conference on Image Processing. IEEE, 2000.

[3] MONGA V, VATS D, EVANS B L. Image Authentication Un-

der Geometric Attacks Via Structure Matching[C]// IEEE International Conference on Multimedia & Expo. IEEE,2005.

[4] ROY S,SUN Q. Robust Hash for Detecting and Localizing Image Tampering[C]// IEEE International Conference on Image Processing. IEEE,2007.

[5] AHMED F,SIYAL M Y,ABBAS V U. A secure and robust hash-based scheme for image authentication[J]. Signal Processing,2010,90(5):1456-1470.

[6] LU W,WU M. Multimedia forensic hash based on visual words [C]// IEEE International Conference on Image Processing. IEEE,2010.

[7] BATTIATO S,FARINELLA G M,MESSINA E,et al. Robust image alignment for tampering detection[J]. IEEE Transactions on Information Forensics and Security,2012,7(4):1105-1117.

[8] LV X,WANG Z J. Perceptual Image Hashing Based on Shape Contexts and Local Feature Points[J]. IEEE Transactions on Information Forensics and Security,2012,7(3):1081-1093.

[9] ZHAO Y,WANG S,ZHANG X,et al. Robust Hashing for Image Authentication Using Zernike Moments and Local Features [J]. IEEE Transactions on Information Forensics and Security, 2013,8(1):55-63.

[10] WANG X,PANG K,ZHOU X,et al. A Visual Model-Based Perceptual Image Hash for Content Authentication[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7):1336-1349.

[11] YAN C P,PUN C M,YUAN X C. Multi-scale image hashing using adaptive local feature extraction for robust tampering detection[J]. Signal Processing,2016,121(C):1-16.

[12] TANG Z,ZHANG X,LI X,et al. Robust Image Hashing with Ring Partition and Invariant Vector Distance[J]. IEEE Transactions on Information Forensics and Security,2017,11(1):200-214.

[13] PUN C M,YAN C P,YUAN X C. Image Alignment based Multi-Region Matching for Object-level Tampering Detection [J]. IEEE Transactions on Information Forensics and Security, 2017,12(2):377-391.

[14] YAN C P,PUN C M,YUAN X C. Quaternion-based Image Hashing for Adaptive Tampering Localization[J]. IEEE Transactions on Information Forensics and Security,2016,11(12): 2664-2677.

[15] YAN C P,PUN C M. Multi-Scale Difference Map Fusion for Tamper Localization using Binary Ranking Hashing[J]. IEEE Transactions on Information Forensics & Security, 2017, PP(99):2144-2158.

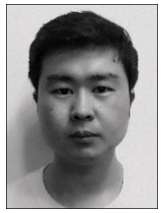
[16] LIU C,LING H,ZOU F,et al. Nonnegative sparse locality preserving hashing[J]. Information Sciences,2014,281:714-725.

[17] ZHANG W,LIU Y,DAS S K,et al. Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach [J]. Pervasive and Mobile Computing, 2008,4(5):658-680.

[18] ELL T A,SANGWINE S J. Hypercomplex Fourier Transforms of Color Images[J]. IEEE Transactions on Image Processing, 2007,16(1):22-35.

[19] BATTIATO S,FARINELLA G M,MESSINA E,et al. Understanding geometric manipulations of images through bovw-based hashing[C]// 2011 IEEE International Conference on Multimedia and Expo(ICME 2011). IEEE Computer Society,2011.

[20] GUO C,MA Q,ZHANG L. Spatio-temporal Saliency detection using phase spectrum of quaternion fourier transform[C]// 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition(CVPR 2008). Anchorage, Alaska, USA. IEEE,2008.



SHANG Jin-yue, born in 1993, postgraduate. His main research interests include image processing and pattern recognition.

BI Xiu-li, born in 1982, Ph.D, associate professor, is a member of China Computer Federation. Her main research interests include digital image processing and multimedia information security.