基于解压缩模块的JPEG同步重压缩检测

王金伟[1],胡冰涛[1],张家伟[1],马 宾[2],罗向阳[3]
(1. 南京信息工程大学计算机学院、网络空间安全学院,江苏南京 210044;2. 齐鲁工业大学山东省计算机网络重点实验室,山东济南 250353;3. 数学工程与高级计算国家重点实验室,河南郑州 450001)

摘 要: 现有的基于深度学习的同步JPEG(Joint Photographic Experts Group)重压缩检测算法大多使用解压缩过程中产生的截断和舍入误差作为分类依据,在检测框架前都存在降低特征提取难度的预处理层,无法实现端到端. 同时,现有的量化底表是根据人为经验所设计的,无法取得解压缩过程的最优解,限制了JPEG重压缩检测算法的精度上限. 针对这些问题,本文提出了一种基于解压缩模块的JPEG重压缩检测方法,该方法利用卷积模拟JPEG解压缩过程,设计了解压缩模块,将JPEG解压缩过程并入网络中从而实现端到端,省去了繁重的预处理步骤;同时,利用深度学习能够自动优化参数的特性,自动去寻找解压缩过程的最优解,减少了由于人工处理导致的图像信息的二次损失,进一步提升了JPEG重压缩检测算法的性能上限. 实验结果表明,本文所提出的JPEG同步重压缩检测算法在超过半数的实验组上都取得了较好的取证表现,在UCID数据集上比现有方法平均精度最多提高1.8%.

关键词: 数字图像取证;卷积神经网络;JPEG重压缩;解压缩模块

基金项目: 国家自然科学基金(No.62072250,No.62172435,No.U1804263,No.U20B2065,No.61872203,No.71802110,No.61802212);中原科技创新领军人才项目(No.214200510019);江苏省自然科学基金(No.BK20200750);河南省网络空间态势感知重点实验室开放基金(No.HNTS2022002);江苏省研究生研究与实践创新项目(No.KYCX200974);广东省信息安全技术重点实验室开放项目(No.2020B1212060078);山东省计算机网络重点实验室开放课题基金(No.SDKLCN-2022-05);人文社会科学教育部项目(No.19YJA630061);江苏高校优势学科建设工程项目

中图分类号: TP751.1 **文章编号:** 0372-2112(2023)04-0850-10

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220424

JPEG Synchronous Double Compression Detection Based on Decompression Module

WANG Jin-wei[1], HU Bing-tao[1], ZHANG Jia-wei[1], MA Bin[2], LUO Xiang-yang[3]
(1. *School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, Jiangsu* 210044, *China*;
2. *Shandong Provincial Key Laboratory of Computer Networks, Qilu University of Technology, Jinan, Shandong* 250353, *China*;
3. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan* 450001, *China*)

Abstract: Most of the existing deep learning-based synchronous JPEG (Joint Photographic Experts Group) double compression detection algorithms use the truncation and rounding errors generated in the decompression process as the classification basis. Pre-processing layers that reduce the difficulty of feature extraction are present before the detection framework, and end-to-end detection cannot be achieved. Meanwhile, the existing quantization base table is designed based on human experience and cannot obtain the optimal solution for the decompression process, which limits the accuracy of the JPEG double compression detection algorithms. To address these issues, a JPEG double compression detection method based on a decompression module is proposed. The proposed method exploits convolution to simulate the JPEG decompression process, and designs the decompression module to incorporate the JPEG decompression process into the network to achieve end-to-end detection, which is free from laborious pre-processing steps. At the same time, the optimal solution for the decompression process is automatically searched based on the self-optimized characteristic of deep learning, which can reduce the secondary loss of image information caused by manual processing and further improve the performance of the JPEG double compression detection algorithm. The experimental results show that the proposed synchronous JPEG double compression detection algorithm achieves better forensic performance in more than half of the experimental groups, with an

收稿日期:2022-04-18;修回日期:2022-10-10;责任编辑:朱梅玉

average accuracy improvement of up to 1.8% over against the existing methods on the UCID dataset.

Key words: digital image forensics; convolutional neural network; double JPEG compression; decompression module

Foundation Item(s): National Natural Science Foundation of China (No.62072250, No.62172435, No.U1804263, No.U20B2065, No.61872203, No.71802110, No.61802212); Zhongyuan Science and Technology Innovation Leading Talent Project of China (No.214200510019); Natural Science Foundation of Jiangsu Province (No.BK20200750); Open Foundation of Henan Key Laboratory of Cyberspace Situation Awareness (No.HNTS2022002); Post Graduate Research & Practice Innvoation Program of Jiangsu Province (No.KYCX200974); Opening Project of Guangdong Province Key Laboratory of Information Security Technology (No.2020B1212060078); Open Project Fund of Shandong Provincial Key Laboratory of Computer Network (No.SDKLCN-2022-05); Ministry of Education of Humanities and Social Science Project (No.19YJA630061); Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) Fund

1　引言

图像处理技术和编辑工具的飞速发展使数字图像的处理变得十分简单,也导致人眼无法分辨图像是否被修改过. 当通过视觉无法分辨篡改图像和原始图像时,就会引发一些潜在的危害,这给新闻、法律、政治等领域都带来了巨大的挑战[1]. 数字图像取证技术因此应运而生[2~4].

重压缩检测在数字图像取证中起着至关重要的作用. 在传感器成像过后,为了方便存储,会将图像压缩保存,而篡改者在对图像进行篡改过后再次存储时,很可能再次将图像压缩保存. 因此,图像是否经历过重压缩可以作为判断图像是否可能被篡改的重要依据.

JPEG(Joint Photographic Experts Group)格式具有存储空间小、传输便捷等特性,作为一种经典的图像压缩格式,被广泛应用于日常生活中,因此,大多数取证任务都与JPEG图像有关. 针对JPEG图像的重压缩检测问题,目前根据使用的量化矩阵是否相同可以分为同步和异步两类问题. 在异步重压缩检测问题上,依赖DCT(Discrete Cosine Transform)系数统计,尤其是DCT系数直方图,人们已经提出了许多基于手工提取特征的算法[5~13]. 相较于异步而言,同步重压缩检测问题由于两次压缩的量化矩阵完全相同,在取证上更有难度. 已经有一些针对JPEG同步重压缩问题的算法被提出[14~22],但这项任务仍然具有挑战性,现有的方法存在两个问题.

首先,无论是传统还是深度学习方法,都依赖截断和舍入误差作为取证特征,需要人工对两种误差进行手动提取,这导致图像空间域信息的二次损失,例如,在提取截断和舍入误差时,使用截断和舍入操作前的图像减去截断和舍入操作后的图像得到误差图像,那么在相减的过程中,就会忽略图像的本体信息. 其次,截断和舍入误差的提取需要对JPEG图像进行解压缩,而现有的解压缩过程中的反量化步骤所使用的量化表是根据经验人为设计的,并不是最优解,这导致JPEG图像的特征未被充分挖掘,限制了现有取证算法的精度上限.

为了解决上述问题,本文提出利用卷积操作模拟JPEG的解压缩过程,从而实现解压缩模块的设计,该模块能够并入网络参与整体训练,通过网络的自动优化寻找解压缩过程的最优解,同时,还能充分挖掘JPEG图像的特征,既能提取到截断和舍入误差这部分特征,又能充分利用JPEG图像的空间域信息. 并且,本文在此基础上提出一个基于解压缩模块的JPEG同步重压缩检测模型,对JPEG同步重压缩问题进行取证. 本文的主要贡献有以下几点.

(1)完成解压缩模块的设计与实现,利用卷积操作模拟JEPG的解压缩过程,该模块能够并入后续检测模型参与整体训练,从而使用网络的自动优化寻找解压缩过程的最优解,解除对JPEG同步重压缩问题的性能限制.

(2)提出一个端到端的基于解压缩模块的JPEG同步重压缩检测模型,省去了烦琐的预处理步骤,同时解决了图像信息的二次损失问题,不仅能够提取到截断和舍入误差特征,还能够充分利用JPEG图像的空间域信息,从而进一步提升JPEG同步重压缩检测精度.

(3)贡献了一个数据集. 该数据集由我们自行拍摄、收集、制作,包含1 000张未压缩的TIF(Tag Image File)格式图像,图像分辨率为6 000×4 000,命名为Nuist-v1(Nanjing University of Information Science and Technology-version 1). 由于现有的JPEG公开数据库都比较陈旧,在各类公开数据库上验证完所提方法的性能后,还在我们自己制作的数据库上再次验证了所提方法的有效性.

2　相关工作

在JPEG同步重压缩检测领域,已经有一些方法取得了比较不错的效果. 下面对这些方法进行一个简要的介绍.

Huang等[14]首先提出了一种方法来检测具有相同量化矩阵的JPEG重压缩图像. 由于非零JPEG系数的数量随着压缩次数的增加而减少,因此使用随机扰动

策略来获得检测双重压缩的阈值. 上述过程重复多次计算平均阈值,可以消除阈值的特殊性. 该方法的关键是确定要修改的JPEG系数的数量. 在此基础上,Li等[15]通过限制干扰的符号来优化干扰噪声.

Yang等[17]提出了一种经典的方法来检测相同量化矩阵的JPEG重压缩问题,并获得了良好的精度. 将离散余弦逆变换系数分成8×8块,以获得包含截断误差和舍入误差的误差块. 如果误差块的最大值超过0.5,则错误块定义为截断错误块;否则,误差块被定义为舍入误差块. 在空间域和DCT域分别计算截断误差块和舍入误差块的均值和方差. 在支持向量机中使用特征来检测具有相同量化矩阵的双JPEG压缩. 在此基础上,Sun[18]设计了一个有预处理的CNN(Convolution Neural Network)架构. 他们将图像进行多次的压缩和解压缩操作,从中提取截断和舍入误差图像作为网络的输入,进而分辨单压缩和重压缩图像.

Huang等[20]也使用由截断和舍入误差组成的误差图像. 考虑到单压缩和重压缩图像之间的统计差异很小,他们使用了密集卷积神经网络来提取特征从而对重压缩问题进行检测.

Wang等[21]发现彩色图像的JPEG压缩和解压缩中的颜色空间转换会导致转换误差的产生,由于转换误差的值是随机的,无规律可循,他们因此采用了转换误差的数量. 此外,截断误差还包含一些无效信息. 球坐标被引入使无效信息变得有效并获得更为明显的特征. 最后使用支持向量机从球坐标和转换误差中提取的特征里来检测具有相同量化矩阵的JPEG重压缩图像.

Deshpande等[22]提出了一种基于量化DCT系数差异的新特征,该特征对图像或图像块的大小相对不变. 基于后续压缩阶段JPEG图像之间不同量化DCT系数的数量,他们设计了一个新的特征向量与前人提出的13维特征EBSF(Error Block Statistical Feature)相连,通过多层感知机MLP(MultiLayer Perceptron)网络学习,将UCID[23](UnCompressed Image Dataset)数据集上的多个斑块大小和质量因子的结果与现有方法进行比较,本文方法在较小尺寸的图像块(128×128),质量因子为60的实验组上,精度最多提高了1.52%.

对于JPEG同步重压缩检测而言,截断和舍入误差是公认的最优秀的取证特征. 在基于深度学习的同步JPEG重压缩算法里,包含预处理层是一个常见的现象,研究者需要在预处理阶段来人工提取截断和舍入误差降低特征提取的难度,而对截断和舍入误差的提取,目前也只能通过人工操作来获取. 即使有一些算法利用卷积去模拟了JPEG压缩过程中的DCT步骤,将DCT层并入了网络,也仅仅是为了方便自动获取DCT系数,而且JPEG的压缩过程与解压缩过程看似是互为逆过程的关系,但是从实际操作来说,并不完全等价,因此,对于JPEG解压缩过程的模拟还处于空白.

现有的基于深度学习的JPEG同步重压缩检测算法存在以下不足:(1)特征过于依赖截断和舍入误差,只能靠人工在预处理阶段提取,导致无法实现端到端;(2)现有的解压缩过程是根据经验人为设计的,存在图像信息的二次损失,并非最优解,这限制了模型精度的进一步提升.

3 先验知识

截断和舍入误差[24]在JPEG解压缩过程[25]中产生,由于数字图像在空间域中像素值都是整数且取值范围在[0,255]之间,而离散余弦逆变换将图像从频率域转换到空间域后产生的IDCT(Inverse Discrete Cosine Transform)系数存在诸多浮点数且部分会超出[0,255]取值范围,因此为了后续步骤的有效进行,需要在离散余弦逆变换之后对IDCT系数进行截断操作和四舍五入操作,这两种操作就会导致截断和舍入误差的产生.

具体来说,当IDCT系数小于0或者大于255时,需要将IDCT系数分别截断为0和255,截断后得到的IDCT系数和截断前的IDCT系数的差值被称为截断误差;同理,当IDCT系数处于[0,255]之间时,需要将浮点数的IDCT系数取整到最近邻的整数,取整操作也就是四舍五入,四舍五入之后得到的IDCT系数与四舍五入之前的IDCT系数之间的差值被称作舍入误差.

截断和舍入误差也是现有JPEG重压缩检测算法最常用的特征之一,无论传统的还是基于深度学习的方法,都是通过人工操作获取截断和舍入误差图像,方法如图1所示.

将误差图像定义为RE_n,用公式可以表示为

$$\mathrm{RE}_n=\mathrm{RTO}\left(\mathrm{IDCT}\left(D_n\right)\right)-\mathrm{IDCT}(D_n) \tag{1}$$

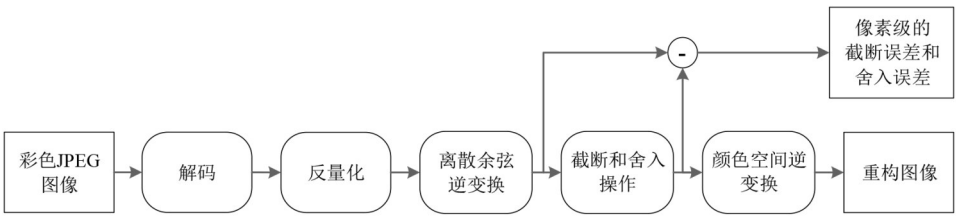

图1 像素级截断误差和舍入误差的获取

其中,RTO为JPEG解压缩中的截断和舍入操作,D_n是反量化后的图像,定义为

$$D_n = \boldsymbol{K}_n \odot Q \tag{2}$$

其中,⊙代表矩阵哈达玛积,$\boldsymbol{K}_n$代表JPEG系数,Q代表对应的量化表中的量化步长. 经过上述操作,便可以人为获取到截断和舍入误差的误差图像.

4　所提方法

在JPEG同步重压缩检测问题中,人工提取截断和舍入误差会带来图像信息二次损失和非端到端等问题. 因此,为了将JPEG解压缩过程并入神经网络模型以实现一体化训练,本文提出了一种端到端的JPEG同步重压缩检测模型,该模型能够自动提取包括截断和舍入误差在内的图像空域信息.

由于JPEG解压缩过程中反量化这一步针对亮度和色度通道分别对应两种不同的量化表,因此本文的网络前半部分设计成双流的结构,将输入网络的通道数为3的JPEG图像拆分成一个通道数为1的亮度图像和一个通道数为2的色度图像,并分别传入两个流中以实现解压缩,同时分别提取亮度信息和色度信息中的不同特征,然后再进行双流的特征聚合,同时引入统计特征,因为统计特征已经在之前的工作中被证明能够有效地提升重压缩检测问题的检测精度. 这里选择的统计特征为特征图整体像素值的均值和方差,从而引导网络关注图像像素值本身的变化. 从图像像素值的变化幅度以及图像像素值整体的分布差异中寻找重压缩所引入的痕迹,同时忽略图像内容差异所带来的影响,在统计层之后,将提取到的特征送入一个由两层全连接层构成的分类器,分类器最后一层输出的是网络对于输入图像是否为JPEG同步重压缩的判别结果. 详细来说,由于JPEG同步重压缩检测属于一种二分类问题,因此分类器的最后一层由两个节点构成. 利用softmax函数将两个节点的输出映射到(0,1)区间,分别代表该输入图像是否为JPEG同步重压缩图像的概率,并依据概率大小进行最终的判断. 本文采用了交叉熵(cross entropy)作为目标损失函数,并依据该损失函数不断优化网络参数,交叉熵损失loss可以表示为

$$\begin{aligned}\text{loss} &= \frac{1}{N}\sum_i L_i \\ &= \frac{1}{N}\sum_i -\left[y_i \cdot \log\left(p_i\right) + (1-y_i)\cdot \log\left(1-p_i\right)\right]\end{aligned} \tag{3}$$

其中,y_i表示样本i的标签,正类(JPEG同步重压缩图像)为1,负类(非JPEG同步重压缩图像)为0;p_i为样本i分类为正类的概率;N为样本总数. 整体的检测模型的结构如图2所示.

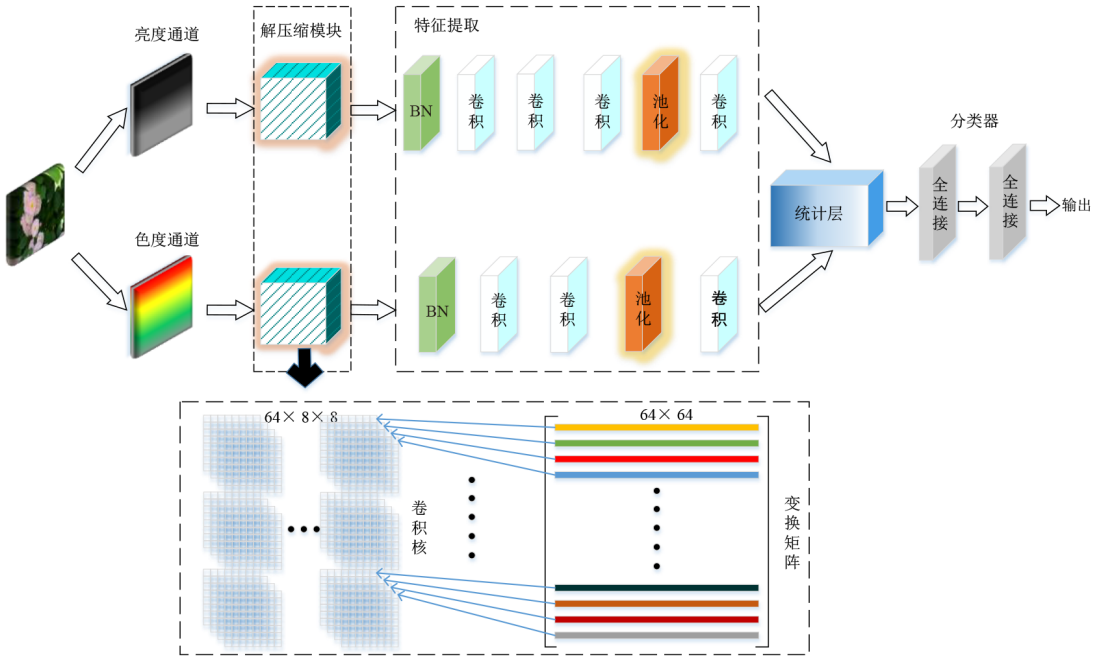

图2　基于解压缩模块的JPEG同步重压缩检测模型

4.1　解压缩模块

4.1.1　利用IDCT变换矩阵实现IDCT

本文利用矩阵乘法实现了IDCT,如图3所示. 先将反量化后得到的每个8×8的图像块拉伸成长度为64的一维列向量,从而得到一个64×256大小的新矩阵. 给新图像矩阵左乘一个IDCT变换矩阵,从而实现对原图像的IDCT变换.

如式(3)所示,假设反量化后经变形得到的新图像

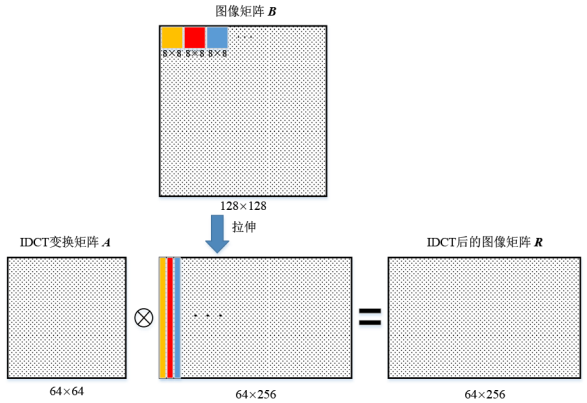

图3 利用IDCT变换矩阵实现IDCT的方式

矩阵为$\boldsymbol{B}$,IDCT变换矩阵为$\boldsymbol{A}$,则有

$$\boldsymbol{R}=\boldsymbol{A}\otimes\boldsymbol{B} \tag{4}$$

其中,⊗代表矩阵叉乘,$\boldsymbol{R}$为反量化后的图像矩阵$\boldsymbol{B}$经过IDCT变换以后得到的图像矩阵.

4.1.2 将量化表与IDCT变换矩阵整合的理论推导

现有的JPEG压缩方法及标准[26,27]中,反量化及IDCT操作是JPEG解压缩流程中独立的两个步骤. 其中,Malvar等人[26]证明了4×4大小的块代替8×8大小的块进行离散余弦变换能够有效降低变换和量化操作复杂度. 不同于Malvar等人的方法,本文拟将反量化与IDCT变换操作整合,并用整合后的系数初始化卷积核的参数,以此实现解压缩参数的自适应学习和更新,从而更好地提取重压缩特征,具体推导过程如下.

在JPEG解压缩过程中,图像块和量化表的大小都为8×8,IDCT变换矩阵的大小为64×64,为了方便推导,本文使用2×2大小和4×4大小的矩阵分别在推导中代替图像块和量化表以及IDCT变化矩阵. 假设有图像块$\boldsymbol{X}$,量化表$\boldsymbol{Y}$,IDCT变换矩阵$\boldsymbol{Z}$,则

$$\boldsymbol{X}=\begin{bmatrix}x_{11}&x_{12}\\x_{21}&x_{22}\end{bmatrix} \tag{5}$$

$$\boldsymbol{Y}=\begin{bmatrix}y_{11}&y_{12}\\y_{21}&y_{22}\end{bmatrix} \tag{6}$$

$$\boldsymbol{Z}=\begin{bmatrix}z_{11}&z_{12}&z_{13}&z_{14}\\z_{21}&z_{22}&z_{23}&z_{24}\\z_{31}&z_{32}&z_{33}&z_{34}\\z_{41}&z_{42}&z_{43}&z_{44}\end{bmatrix} \tag{7}$$

反量化操作后得到哈达玛积为

$$\boldsymbol{X}\odot\boldsymbol{Y}=\begin{bmatrix}x_{11}y_{11}&x_{12}y_{12}\\x_{21}y_{21}&x_{22}y_{22}\end{bmatrix} \tag{8}$$

将反量化操作得到的结果拉伸成向量,拉伸操作记为$\oint$,则有

$$\oint_{\boldsymbol{X}\odot\boldsymbol{Y}}=\begin{bmatrix}x_{11}y_{11}\\x_{12}y_{12}\\x_{21}y_{21}\\x_{22}y_{22}\end{bmatrix} \tag{9}$$

对拉伸之后的矩阵进行IDCT操作,得到:

$$\boldsymbol{Z}\otimes\left(\oint_{\boldsymbol{X}\odot\boldsymbol{Y}}\right)=\begin{bmatrix}z_{11}&z_{12}&z_{13}&z_{14}\\z_{21}&z_{22}&z_{23}&z_{24}\\z_{31}&z_{32}&z_{33}&z_{34}\\z_{41}&z_{42}&z_{43}&z_{44}\end{bmatrix}\otimes\begin{bmatrix}x_{11}y_{11}\\x_{12}y_{12}\\x_{21}y_{21}\\x_{22}y_{22}\end{bmatrix}$$

$$=\begin{bmatrix}z_{11}x_{11}y_{11}+z_{12}x_{12}y_{12}+z_{13}x_{21}y_{21}+z_{14}x_{22}y_{22}\\z_{21}x_{11}y_{11}+z_{22}x_{12}y_{12}+z_{23}x_{21}y_{21}+z_{24}x_{22}y_{22}\\z_{31}x_{11}y_{11}+z_{32}x_{12}y_{21}+z_{33}x_{21}y_{21}+z_{34}x_{22}y_{22}\\z_{41}x_{11}y_{11}+z_{42}x_{12}y_{12}+z_{33}x_{21}y_{21}+z_{44}x_{22}y_{22}\end{bmatrix} \tag{10}$$

将量化表和IDCT变换矩阵进行整合,进而得到一个一步实现反量化及IDCT操作的变换矩阵,记为$\boldsymbol{L}$. 首先,定义一种矩阵变形操作,记为$\int$,则对量化表$\boldsymbol{Y}$进行变形,得到:

$$\int_{\boldsymbol{Y}}=\begin{bmatrix}y_{11}&y_{12}&y_{21}&y_{22}\\y_{11}&y_{12}&y_{21}&y_{22}\\y_{11}&y_{12}&y_{21}&y_{22}\\y_{11}&y_{12}&y_{21}&y_{22}\end{bmatrix} \tag{11}$$

将变形后的量化表与IDCT变换矩阵求哈达玛积,得到:

$$\boldsymbol{L}=\int_{\boldsymbol{Y}}\boldsymbol{Z}=\begin{bmatrix}y_{11}&y_{12}&y_{21}&y_{22}\\y_{11}&y_{12}&y_{21}&y_{22}\\y_{11}&y_{12}&y_{21}&y_{22}\\y_{11}&y_{12}&y_{21}&y_{22}\end{bmatrix}\odot\begin{bmatrix}z_{11}&z_{12}&z_{13}&z_{14}\\z_{21}&z_{22}&z_{23}&z_{24}\\z_{31}&z_{32}&z_{33}&z_{34}\\z_{41}&z_{42}&z_{43}&z_{44}\end{bmatrix}$$

$$=\begin{bmatrix}y_{11}z_{11}&y_{12}z_{12}&y_{21}z_{13}&y_{22}z_{14}\\y_{11}z_{21}&y_{12}z_{22}&y_{21}z_{23}&y_{22}z_{24}\\y_{11}z_{31}&y_{12}z_{32}&y_{21}z_{33}&y_{22}z_{34}\\y_{11}z_{41}&y_{12}z_{42}&y_{21}z_{43}&y_{22}z_{44}\end{bmatrix} \tag{12}$$

将变换矩阵$\boldsymbol{L}$与拉伸后的图像块$\oint_{\boldsymbol{X}}$相乘,得到:

$$\boldsymbol{L}\otimes\oint_{\boldsymbol{X}}=\begin{bmatrix}y_{11}z_{11}&y_{12}z_{12}&y_{21}z_{13}&y_{22}z_{14}\\y_{11}z_{21}&y_{12}z_{22}&y_{21}z_{23}&y_{22}z_{24}\\y_{11}z_{31}&y_{12}z_{32}&y_{21}z_{33}&y_{22}z_{34}\\y_{11}z_{41}&y_{12}z_{42}&y_{21}z_{43}&y_{22}z_{44}\end{bmatrix}\otimes\begin{bmatrix}x_{11}\\x_{12}\\x_{21}\\x_{22}\end{bmatrix}$$

$$=\begin{bmatrix}z_{11}x_{11}y_{11}+z_{12}x_{12}y_{12}+z_{13}x_{21}y_{21}+z_{14}x_{22}y_{22}\\z_{21}x_{11}y_{11}+z_{22}x_{12}y_{12}+z_{23}x_{21}y_{21}+z_{24}x_{22}y_{22}\\z_{31}x_{11}y_{11}+z_{32}x_{12}y_{21}+z_{33}x_{21}y_{21}+z_{34}x_{22}y_{22}\\z_{41}x_{11}y_{11}+z_{42}x_{12}y_{12}+z_{33}x_{21}y_{21}+z_{44}x_{22}y_{22}\end{bmatrix} \tag{13}$$

我们发现$\boldsymbol{Z}\otimes\left(\oint_{\boldsymbol{X}\odot\boldsymbol{Y}}\right)=\boldsymbol{L}\otimes\oint_{\boldsymbol{X}}$,此规律可以推

广到n阶矩阵的情况. 有一个任意的n阶矩阵$\boldsymbol{G}$,以及两个任意的m阶矩阵$\boldsymbol{H},\boldsymbol{K}$,其中,$m=\sqrt{n}$,可以得到:

$$\boldsymbol{G}\otimes\left(\oint_{\boldsymbol{H}\odot\boldsymbol{K}}\right)=\int_{\boldsymbol{K}}\odot\boldsymbol{G}\otimes\oint_{\boldsymbol{H}} \tag{14}$$

综上所述,对于JPEG解压缩过程,可以使用整合后的变换矩阵$\boldsymbol{L}$中每一行的64个元素去初始化一个8×8的卷积核,因此本文使用了64个8×8的卷积核实现了通过卷积模拟JPEG解压缩过程.

4.2　特征提取模块

特征提取过程分布到整体检测模型的两个流中去分别完成. 由于解压缩过程需要对图像的亮度通道和色度通道分别进行反量化操作,因此为了满足实际的需要,图像在输入时就将亮度通道和色度通道分离开来,分别送入两个流中进行特征提取. 两个流中分别实现亮度信息和色度信息的分离式提取之后,再对提取到的特征进行聚合.

亮度通道流中由一个BN(Batch Normalization)层、四个卷积层和一个池化层组成. 其中BN层主要进行数据的归一化操作从而加速网络的收敛以及防止过拟合现象的出现;池化层在这里选择最大池化层,并且将池化窗口的大小设置为2×2,池化步长也为2×2;卷积层的卷积核大小都为3×3,卷积核数量依次递增,分别为16,32,64,128个.

色度通道流中的架构与亮度通道流有些许不同,由一个BN层、三个卷积层和一个池化层组成. 其中BN层与池化层的设计与亮度通道中的一致;而卷积层层数减少了一层,卷积核大小设置为5×5,卷积核个数依次递增,分别为16,32,64个. 这样设计是因为压缩对色度通道的信息损失很严重,色度信息远少于亮度信息,如果使用同样多的卷积层去提取特征可能会造成特征冗余,同时,由于信息量较少,如果卷积核设置过小可能会提取不到有效信息. 为了充分提取色彩特征,本文对色度通道进行了上述设计.

4.3　统计层

统计层里沿用了统计特征这一优秀的取证特征,选择传统的均值和方差作为本文的分类依据. 设像素总数为T,第i个像素的值为x_i,则传统均值和方差的计算方法如式(14)和式(15)所示:

$$E(x)=\frac{1}{T}\sum_{i}^{T}x_i \tag{15}$$

$$V(x)=\frac{1}{T}\sum_{i=1}^{T}\left(x_i-E(x)\right)^2 \tag{16}$$

统计特征能够反映图像像素值本身在统计意义上的分布特点. 使用统计层将提取到的特征转换为统计特征是为了引导模型去关注图像像素值本身的变化,从而发现重压缩所引入的痕迹,继而对单压缩和重压缩进行取证.

5　实验

本节通过消融实验去验证了本文所提方法中解压缩模块和统计层这两个部分的有效性. 同时,在我们自己建立的数据集NUIST-v1以及公用数据库UCID,NRCS[28](Natural Resources Conservation Service)上分别测试了所提方法检测JPEG重压缩问题的有效性,并且与几种现有的JPEG重压缩检测算法进行了对比.

5.1　实验细节

5.1.1　数据集

Nuist-v1数据集由一架Sony a6300相机收集并制作而成. 它由1 000张分辨率为6 000×4 000的TIF格式的彩色图像构成. 场景类型为南京信息工程大学校内的建筑物、花草树木、公共设施、行人等. 由于图像尺寸很大,在此次实验过程中,首先将这些大尺寸图像划分共计为230 000张尺寸为256×384不重复的小尺寸图像;其次,选择其中图像内容丰富的7 000张图像并以5∶2的比例划分为训练集和测试集. 在选择完毕后,将5 000张用于制作训练集的图像分别以{20,30,40,50,60,70,80,90}的质量因子进行单次压缩和二次压缩形成训练集的正类样本以及负类样本,将2 000张用于制作测试集的图像分别以{20,30,40,50,60,70,80,90}的质量因子进行单次压缩和二次压缩形成测试集的正类样本和负类样本,最终构成此次试验的实验数据.

UCID数据集目前包含1 338张尺寸为512×384的未压缩的TIFF图像,涉及各种主题,包括室内和室外的自然场景和人造物体. 所有图像都是用美能达数码彩色相机拍摄的,并且所有参数都设置成自动模式以模仿平日普通人摄影的习惯.

NRCS数据集全称为自然资源/农业形象数据库,是由USDA(United States Department of Agriculture)自然资源保护局所建立的. 它里面包含959张尺寸为1 800×2 800,从美国的不同州以及不同区域选择的自然图像和农业图像

在公开数据集的实验中,本文首先将这两个数据库中的图像尺寸裁剪为256×384,其次对这些图像进行单压缩和重压缩以形成正类样本和负类样本,最后按照5∶2的比例划分训练集与测试集以满足实验的需要.

混合数据集MIXDATA由NUIST-v1,UCID和NRCS数据集中的图像混合而成,三种数据库中的图像尺寸不一致,因此需要统一图像尺寸. 由于resize操作是根据特定插值算法(例如,最邻近插值)重新计算目标图像各个像素位置的像素值,这种操作会影响到原始图像的像素值分布,也会干扰JPEG同步重压缩特征的提

取,因此本文使用了更加合适的裁剪操作作为统一图像尺寸的手段. 本文统一将三个数据集上的图像裁剪成尺寸为256×384的图像块,按照每个数据集各1 000张的比例混合而成. 3 000张图像块中,2 000张用于制作训练集,1 000张用于制作测试集.

5.1.2 实验设置

在数据准备中,对事先准备的由量化表和IDCT变换矩阵整合得到的新变换矩阵进行读取,这里读取的是分别为亮度量化表整合以及色度量化表整合的两种变换矩阵,在读取完毕之后,使用这两种变换矩阵分别初始化检测模型两流前端的解压缩模块.

输入图像的大小调整为256×384×3,在进入网络后会被分割成1张通道数为1的亮度图像和1张通道数为2的色度图像(亮度图像由源图像的Y通道构成,色度图像由源图像的Cb和Cr通道构成),然后分别送入模型的两个流中以提取特征.

该模型的批次大小设置为50,即每次输入50张图像进入网络进行训练. 整个网络由Adam优化,学习率设置为10^{-5},一阶矩估计的指数衰减因子(beta_1)设置为0.5. 训练轮次(epoch)经过实验验证确定在350结束. 所有的实验都在一张NVIDA 1080Ti GPU上完成.

5.1.3 模型参数

整体检测模型由九个卷积层(包含解压缩模块中的两个卷积层)、两个BN层、两个池化层、一个统计层和两个全连接层构成. 其中,解压缩模块由包含64个8×8卷积核且卷积核参数被变换矩阵初始化的卷积层组成;BN层主要是为了加速网络训练和收敛的速度并防止过拟合现象的出现;池化层选择使用滑动窗口大小为2×2且步长为2的最大池化层;亮度通道流中卷积层卷积核大小都设置为3×3,但卷积核的个数分别为16,32,64,128;色度通道流中卷积层卷积核大小都设置为5×5;统计层中选择将特征提取到的特征转换为均值和方差这两种统计特征;分类器包含两层全连接层,神经元个数分别设置为128和2,从而执行最后的分类操作. 关于网络的详细结构和参数如表1所示.

表1 基于解压缩模块的JPEG同步重压缩检测模型详细参数

层数	亮度通道流				色度通道流			
	层名	核尺寸	步长	输出尺寸	层名	核尺寸	步长	输出尺寸
1	解压缩模块	64×8×8	8×8	32×48×64	解压缩模块	64×8×8	8×8	32×48×64
2	BN层	×	×	32×48×64	BN层	×	×	32×48×64
3	卷积层1	16×3×3	1×1	32×48×16	卷积层1	16×5×5	1×1	32×48×16
4	卷积层2	32×3×3	1×1	32×48×32	卷积层2	32×5×5	1×1	32×48×32
5	卷积层3	64×3×3	1×1	32×48×64	最大池化层	2×2	2×2	16×24×32
6	最大池化层	2×2	2×2	16×24×64	卷积层4	64×3×3	1×1	16×24×64
7	卷积层4	128×3×3	1×1	16×24×128	—	—	—	—
双流合并								
层数	层名	核尺寸		步长		输出尺寸		
8	统计层	—		—		1×384		
9	全连接层1	384×128		—		128		
10	全连接层2	128×2		—		2		

5.2 消融实验

5.2.1 解压缩模块的影响

为了探寻解压缩模块对所提方法在检测JPEG重压缩问题上的性能的影响,本文在Nuist-v1数据集上对完整模型及去除解压缩模块的模型的性能进行了评估. 解压缩模块能够将原本需要在预处理阶段人工操作的JPEG解压缩过程通过卷积模拟的方式并入模型的训练中,从而实现端到端的一体化优化,而实现这一步意味着可以通过深度学习,利用参数的自动优化特性去寻找一个更优的解压缩过程,从而减少由于人工进行解压缩造成的信息损失. 在实验中,我们分别测试了包含解压缩模块和去除解压缩模块的方法在JPEG重压缩检测问题上的性能,对比两者所取得的精度来证明解压缩模块给整体检测模型所带来的积极影响,实验结果如表2所示. 从表2可以看出,在质量因子从20~90的所有实验组中,含有解压缩模块的检测模型整体精度都高于去除解压缩模块的检测模型,整体精度平均提升3.01%. 说明我们的解压缩模块对特征提取的引导作用是非常显著的,能够帮助网络提取到解压缩过程中有利于同步重压缩问题分类的特征.

5.2.2 统计层的影响

为了探寻统计层对于所提方法在检测JEPG重压缩问题上性能的影响,本文在Nuist-v1数据集上对完整模型及去除统计层的模型的性能进行了评估. 在上节中,已经证明了统计特征对JPEG重压缩检测问题有其积极的影响,它们能够在一定程度上排除图像语义信

表2　完整模型和去除解压缩模块模型在JPEG同步重压缩检测上的精度

质量因子(同步)	实验组	
	完整模型/%	去除解压缩模块的模型/%
20	73.36	69.73
30	75.43	71.36
40	76.37	73.31
50	77.85	74.54
60	79.31	77.89
70	84.11	81.55
80	87.95	84.73
90	90.60	87.80
平均精度	80.62	77.61

表3　完整模型和去除统计层的模型在JPEG同步重压缩检测上的精度

质量因子(同步)	实验组	
	完整模型/%	去除解压缩模块的模型/%
20	73.36	72.35
30	75.43	74.60
40	76.37	75.15
50	77.85	75.37
60	79.31	77.86
70	84.11	81.35
80	87.95	86.43
90	90.60	89.57
平均精度	80.62	79.09

息的影响,关注图像像素值本身在整体分布以及细微之处的变化,从而发现重压缩给图像所带来的痕迹,帮助模型发现重压缩和单压缩图像之间的差异,因此在这个工作中我们依然沿用了统计特征这一优秀的取证特征. 具体而言,在这组实验中,我们分别测试了包含统计层的模型和去除统计层模型在JPEG重压缩检测问题上的性能,通过二者性能变化说明统计层对于整体检测模型的积极影响,实验结果如表3所示.

从表3可以看出,在质量因子20~90的所有实验组中,包含统计层的检测模型相比去除统计层的检测模型,精度都有所提高,整体精度平均提升1.53%. 再次说明了统计特征中的均值和方差在JPEG重压缩检测问题中的重要意义,也说明了重压缩引入的痕迹很大程度上存在于图像像素值的整体分布之中.

5.3　JPEG同步重压缩检测效果及对比实验

为了充分说明本文所提出的基于解压缩模块的JPEG重压缩检测方法在JPEG重压缩检测问题上的有效性,我们在自己制作的数据集NUIST-v1、公开数据集UCID和NRCS以及三者的混合库MIXDATA上都对本文提出的检测模型进行了性能测试,同时也与两种最新的基于深度学习的JPEG同步重压缩检测方法[18,22]进行了对比,实验结果如表4所示.

表4　所提方法和现有方法在多个数据库上对于JPEG同步重压缩检测问题的精度　　单位:%

数据集	方法	质量因子							
		20	30	40	50	60	70	80	90
NUIST-v1	本文	**73.36**	**75.43**	**76.37**	**77.85**	79.31	84.11	**87.95**	**90.60**
	Peng[18]	71.50	73.33	74.48	76.43	**79.90**	81.28	83.44	85.15
	Desh[22]	72.33	74.45	75.37	75.17	78.21	**84.45**	85.43	87.58
UCID	本文	**79.16**	81.52	**84.48**	**85.13**	85.40	84.54	**97.25**	**98.36**
	Peng[18]	76.88	**81.85**	83.27	84.55	**85.46**	**86.28**	93.27	96.89
	Desh[22]	76.23	78.98	81.89	83.28	83.12	83.62	96.13	97.34
NRCS	本文	**77.53**	**79.25**	**81.05**	83.14	84.57	86.91	**94.00**	**98.55**
	Peng[18]	74.35	77.37	80.25	81.10	82.00	87.46	90.16	94.46
	Desh[22]	76.68	78.73	79.94	**83.16**	**85.74**	**88.40**	92.34	96.37
MIXDATA	本文	**71.45**	72.60	**73.85**	**74.76**	76.19	78.54	80.16	**84.85**
	Peng[18]	68.58	69.19	71.38	73.67	75.71	**79.69**	81.13	83.37
	Desh[22]	69.92	**73.73**	72.46	74.55	**77.05**	78.36	**82.67**	83.81

从表4可以看出,在NUIST-v1数据集上,本文所提方法在质量因子为{20,30,40,50,80,90}的实验组上的精度都高于所对比的两种方法,在质量因子{60,70}上的表现虽然不是最高,但精度也与两种对比方法接近;在UCID数据集上,所提方法在质量因子为{20,40,50,80,90}的实验组上精度都高于两种对比方法,在质量因子为{30,60,70}的实验组上精度略低;在NRCS数据集上,所提方法在质量因子为{20,30,40,80,90}的实验组上精度都高于两种对比方法,在质量因子为{50,60,70}的实验组精度略低;在混合数据集MIXDATA上,所提方法在质量因子为{20,40,50,90}的实验组上精度都高于两种对比方法,在质量因子为{30,60,70,80}的实验组上精度略低.

综上所述,本文所提方法在超过半数的实验组中

都取得了精度上的优势,在质量因子为{20,30,40,50,80,90}的实验组上表现较好,在质量因子为{60,70}时,检测精度与两种对比方法的效果接近.这是因为在质量因子为80和90时,由于压缩程度较轻,对色度通道的量化步长相对较小,此时色度信息对取证的帮助很大,而在质量因子{20,30,40,50}时,压缩的程度较重,截断和舍入误差的有效性有所降低,此时空域特征大大提升了取证模型的有效性,质量因子60和70时,误差特征具备较强的有效性,所以空域特征的提升有限,甚至造成了一定的特征冗余,从而降低了所提模型的精度.

6 总结

本文分析了现有方法存在依赖人工提取的截断和舍入误差这一问题.为解决这一问题,本文通过公式推导验证了使用卷积模拟JPEG解压缩过程的可行性.在设计的JPEG解压缩模块的基础上,提出了一个新的JPEG同步重压缩检测模型,使JPEG解压缩过程并入了端到端的可训练检测模型,进一步提升了所提JPEG同步重压缩检测算法在解决JPEG同步重压缩问题上的性能.在实验部分,本文通过多组消融实验验证了所提方法各个模块的有效性,同时在我们自己的数据集和公开数据集上通过多组性能测试与现有JPEG重压缩检测方法进行了对比.最后,本文对实验的结果进行了分析,阐明了所提方法的优势,以及目前存在的短板和今后改进的方向.

参考文献

[1] AYABURI E W, TREKU D N. Effect of penitence on social media trust and privacy concerns: The case of Facebook[J]. International Journal of Information Management, 2020, 50: 171-181.

[2] ZHANG Q B, LU W, WENG J. Joint image splicing detection in DCT and Contourlet transform domain[J]. Journal of Visual Communication and Image Representation, 2016, 40: 449-458.

[3] CHEN B J, COATRIEUX G, WU J S, et al. Fast computation of sliding discrete tchebichef moments and its application in duplicated regions detection[J]. IEEE Transactions on Signal Processing, 2015, 63(20): 5424-5436.

[4] LI J, LI X L, YANG B, et al. Segmentation-based image copy-move forgery detection scheme[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 507-518.

[5] LUKÁŠ J, FRIDRICH J. Estimation of primary quantization matrix in double compressed JPEG images[J]. Digital Forensic Research, 2003: 5-8.

[6] POPESCU A C, FARID H. Statistical tools for digital forensics[C]//International Workshop on Information Hiding. Toronto: Springer, 2004: 128-147.

[7] FU D D, SHI Y Q, SU W. A generalized Benford's law for JPEG coefficients and its applications in image forensics[C]//Proceedings of Security, Steganography, and Watermarking of Multimedia Contents IX. San Jose: SPIE, 2007: 574-584.

[8] LI B, SHI Y Q, HUANG J W. Detecting doubly compressed JPEG images by using mode based first digit features[C]//2008 IEEE 10th Workshop on Multimedia Signal Processing. Cairns: IEEE, 2008: 730-735.

[9] AMERINI I, BECARELLI R, CALDELLI R, et al. Splicing forgeries localization through the use of first digit features[C]//2014 IEEE International Workshop on Information Forensics and Security (WIFS). Atlanta: IEEE, 2014: 143-148.

[10] TAIMORI A, RAZZAZI F, BEHRAD A, et al. A novel forensic image analysis tool for discovering double JPEG compression clues[J]. Multimedia Tools and Applications, 2017, 76(6): 7749-7783.

[11] WANG J W, HUANG W, LUO X Y, et al. Non-aligned double JPEG compression detection based on refined Markov features in QDCT domain[J]. Journal of Real-Time Image Processing, 2020, 17(1): 7-16.

[12] YAO H, WEI H B, QIN C, et al. An improved first quantization matrix estimation for nonaligned double compressed JPEG images[J]. Signal Processing, 2020, 170: 107430.

[13] LIU X J, LU W, XUE Y J, et al. Upscaling factor estimation on double JPEG compressed images[J]. Multimedia Tools and Applications, 2020, 79(19): 12891-12914.

[14] HUANG F J, HUANG J W, SHI Y Q. Detecting double JPEG compression with the same quantization matrix[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 848-856.

[15] NIU Y K, LI X L, ZHAO Y, et al. An enhanced approach for detecting double JPEG compression with the same quantization matrix[J]. Signal Processing: Image Communication, 2019, 76: 89-96.

[16] LAI S Y, BÖHME R. Block convergence in repeated transform coding: JPEG-100 forensics, carbon dating, and tamper detection[C]//2013 IEEE International Conference on Acoustics, Speech and Signal Processing. Vancouver: IEEE, 2013: 3028-3032.

[17] YANG J Q, XIE J, ZHU G P, et al. An effective method for detecting double JPEG compression with the same quantization matrix[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(11): 1933-1942.
[18] PENG P, SUN T F, JIANG X H, et al. Detection of double JPEG compression with the same quantization matrix based on convolutional neural networks[C]//2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC). Honolulu: IEEE, 2018: 717-721.
[19] WANG Z F, ZHU L, MIN Q S, et al. Double compression detection based on feature fusion[C]//2017 International Conference on Machine Learning and Cybernetics (ICMLC). Honolulu: IEEE, 2017: 379-384.
[20] HUANG X S, WANG S L, LIU G S. Detecting double jpeg compression with same quantization matrix based on dense cnn feature[C]//2018 25th IEEE International Conference on Image Processing (ICIP). Athens: IEEE, 2018: 3813-3817.
[21] WANG J W, WANG H, LI J, et al. Detecting double JPEG compressed color images with the same quantization matrix in spherical coordinates[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30 (8): 2736-2749.
[22] DESHPANDE A U, HARISH A N, SINGH S, et al. Neural network based block-level detection of same quality factor double JPEG compression[C]//2020 7th International Conference on Signal Processing and Integrated Networks (SPIN). Noida: IEEE, 2020: 828-833.
[23] SCHAEFER G, STICH M. UCID: An uncompressed color image database[C]//Proceedings of Storage and Retrieval Methods and Applications for Multimedia. San Jose: SPIE, 2003: 472-480.
[24] WANG H, WANG J W, LUO X Y, et al. Detecting aligned double JPEG compressed color image with same quantization matrix based on the stability of image[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(6): 4065-4080.
[25] 王昊. 彩色图像同步JPEG重压缩检测研究[D]. 南京: 南京信息工程大学, 2020.
WANG H. Research on Detecting Double JPEG Compressed Image with the Same Quantization Matrix[D]. Nanjing: Nanjing University of Information Science & Technology, 2020. (in Chinese)
[26] MALVAR H S, HALLAPURO A, KARCZEWICZ M, et al. Low-complexity transform and quantization in H.264/AVC[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(7): 598-603.
[27] WALLACE G K. The JPEG still picture compression standard[J]. Communications of the ACM, 1991, 34(4): 30-44.
[28] NRCS Photo Gallery[EB/OL]. (2017-12-07) [2022-04]. http://photogallery.nrcs.usda.gov.

作者简介

王金伟　1978年生,博士、教授、博导. 入选江苏省“333高层次人才培养工程”. 主要研究方向为人工智能安全、彩色图像取证、彩色图像可逆水印、鲁棒水印和图像加密等. 中国电子学会会员编号:E190027579M.

罗向阳(通讯作者)　1978年生,博士、教授、博导,国防科技卓越青年基金获得者,先后入选河南省科技创新杰出青年、杰出人才、中原科技创新领军人才. 主要研究方向为网络与信息安全.
E-mail: xiangyangluo@126.com