采用IWT和自适应伪Zernike矩的鲁棒可逆水印方案

高光勇[1,2],花 锋[1,2],王 敏[1,2],赵传信[3],夏志华[4*]
(1. 南京信息工程大学数字取证教育部工程研究中心,江苏南京 210044; 2. 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; 3. 安徽师范大学计算机与信息学院,安徽芜湖 241002; 4. 暨南大学网络安全学院,广东广州 510632)

摘 要: 鲁棒可逆水印(Robust Reversible Watermarking,RRW)是近年来信息隐藏领域中一个非常新颖和有价值的研究方向,无论是在图像的版权认证还是高保真领域都有较好发展前景. 然而,现有的RRW方案抵抗几何变换、常见攻击以及联合攻击的鲁棒性较差. 为了解决这些问题,本文提出一种采用整数小波变换(Integer Wavelet Transformation,IWT)和自适应伪Zernike矩的鲁棒可逆水印方案,该方案在提升水印不可感知性的同时具有可逆性和鲁棒性. 首先,由原始图像通过IWT得到低频区域计算生成伪Zernike矩的幅度,然后用自适应归一化方法选择合适的矩,再通过改进的带抖动补偿量化索引调制技术将鲁棒水印嵌入到合适的伪Zernike矩中,对带水印的伪Zernike矩进行重构生成水印图像. 最后计算其hash值,并将其与水印图像和原始图像之间的误差、重构误差组成辅助信息嵌入水印图像中,在无攻击的情况下实现载体图像的可逆还原. 实验结果表明,本方案对常见信号处理和几何变换攻击具有鲁棒性,相较于近几年提出的RRW方案,本方案在不可见性下实现了更好的鲁棒性.

关键词: 鲁棒水印;伪Zernike矩;整数小波变换;可逆性;信息隐藏
基金项目: 国家重点研发计划(No.2022YFB3103100);教育部人文社科项目(No.24YJA870002);江苏省研究生科研创新计划项目(No.KYCX22_1221)
中图分类号: TP37 **文献标识码:** A **文章编号:** 0372-2112(2025)05-1571-13
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20240646

A Robust Reversible Watermarking Scheme Using IWT and Adaptive Pseudo-Zernike Moment

GAO Guang-yong[1,2], HUA Feng[1,2], WANG Min[1,2], ZHAO Chuan-xin[3], XIA Zhi-hua[4*]
(1. *Engineering Research Center of Digital Forensics*, *Ministry of Education*, *Nanjing University of Information Science and Technology*, *Nanjing*, *Jiangsu* 210044, *China*; 2. *School of Computer Science and Cyberspace Security*, *Nanjing University of Information Science and Technology*, *Nanjing*, *Jiangsu* 210044, *China*; 3. *School of Computer and Information*, *Anhui Normal University*, *Wuhu*, *Anhui* 241002, *China*; 4. *College of Network Security*, *Jinan University*, *Guangzhou*, *Guangdong* 510632, *China*)

Abstract: Robust reversible watermarking (RRW) is a very novel and valuable research direction in the field of information hiding in recent years, which has a good development prospect in both image copyright authentication and high-fidelity fields. However, existing RRW schemes are less robust against geometric transformations, common attacks, and joint attacks. To solve these issues, this paper proposes a robust reversible watermarking scheme using integer wavelet transformation (IWT) and adaptive Pseudo-Zernike moments that is reversible and robust while improving watermark imperceptibility and embedding capacity. First, the low-frequency region is obtained from the original image through IWT, and the magnitude of the generated Pseudo-Zernike moment is calculated, and then the qualified moment is selected by the adaptive normalization method and the optimized embedding strategy. Then, the robust watermark is embedded into the appropriate Pseudo-Zernike moments by the improved quantization index modulation with distortion compensation (DC-QIM), and the watermarked Pseudo-Zernike moment is reconstructed to generate the watermarked image. Finally, its hash value is calculated, and the error between the watermarked image and the original image and the reconstruction error constitute auxiliary information embedded in the watermark image, so as to realize the reversible restoration of the carrier image without attack.

收稿日期:2024-07-09;修回日期:2025-03-20;责任编辑:朱梅玉
*通讯作者:夏志华

Experimental results show that the proposed scheme is robust to common signal processing and geometric transformation attacks. Compared with RRW schemes proposed in recent years, this scheme achieves better robustness under good invisibility.

Key words: robust watermarking; Pseudo-Zernike moment; integer wavelet transform; reversibility; information hiding

Foundation Item(s): Research and Development Plan of China (No.2022YFB3103100); Humanities and Social Science Foundation of the Ministry of Education (No.24YJA870002); Graduate Research Innovation Program of Jiangsu (No.KYCX22_1221)

1 引言

在如今的信息时代中,数字化产品本身的可复制和易于传播的特性使盗版者只需要复制原始数字作品,就可以在不经版权人的同意进行传播. 同时,对一些重要证件、发票、设计稿及秘密文件的篡改或伪造也变得容易. 这些行为对信息安全有一定的影响,给用户带来极大不便. 因此,数字产品迫切需要有效的手段来保护作品内容,防止侵犯版权. 对此,基于密码学[1,2]的算法应运而生,但是在密码学中如果加密算法遭到破解,信息就会失去保护. 为解决上述问题,信息隐藏技术[3~5]随之出现,其核心是将机密信息隐藏于公共媒体中. 其中,数字水印技术[6,7]是一种既具有鲁棒性又兼具隐蔽性的安全技术手段,主要应用包括版权保护、数据监控和数据跟踪等,为数字图像版权的查证提供了技术支撑. 同时,鲁棒水印和可逆水印[8]相结合有广阔应用前景,既保护数字媒体,又能在未受到攻击时恢复载体的原始状态.

在现实世界中,更多的业务对水印嵌入容量提出了更高要求,水印容量要承载必要的业务信息. 在图像处理中水印的嵌入能力是衡量数字图像处理能力的重要指标,增大有效嵌入容量的同时提升水印对各种攻击的抵抗能力具备现实意义,同时也是一个在研究中难解决的问题. 目前研究中嵌入的水印容量非常有限,提高水印的嵌入容量、如何有效抵抗组合几何攻击,一直是数字水印领域具有挑战性的课题.

基于变换域的图像数字水印算法的研究有效提高了水印的抗干扰能力和隐蔽性. 比如基于离散余弦变换(Discrete Fourier Transform, DCT)[9]和离散小波变换(Discrete Wavelet Transformation, DWT)[10]的研究方案可以很好地抵抗噪声攻击和压缩攻击. 例如,Zhu等人[11]对真实图像基于小波的模拟,其中主要信号由3级小波分解的细节系数构成,对广泛攻击具有更强的鲁棒性,例如值缩放、高斯滤波和加性噪声. Dong等人[12]将可变形网格用于校正攻击引起的变形,然后从校正后的图像中提取水印. 同时,通过使用直接序列码分多址在图像的离散余弦变换域中嵌入多位比特水印,对大范围的几何攻击具有鲁棒性. 在文献[13]中,作者提出了一种鲁棒的水印算法,通过在加密图像中嵌入水印来抵抗JPEG2000压缩. Pereira等人[14]使用傅里叶变换将数字水印嵌入到图像中,实现对一般线性变换和压缩的鲁棒性. Kang等人[15]设计了一种抗仿射变换的水印算法,通过使用复合技术提高对几何失真JPEG压缩的鲁棒性.

为避免传统鲁棒水印方案中的原始图像信息的永久性丢失,研究者们提出了可逆鲁棒水印方法(无失真鲁棒水印). Coltuc等人[16]提出了一种用于图像认证的通用无失真鲁棒水印框架,其中,原始图像和水印图像之间的差异被可逆地嵌入到水印图像中以恢复原始图像. 该方案的2阶段水印方法,给出一个具体情况,将比特嵌入到图像DCT的AC(Alternating Current)系数中,并将失真嵌入到带水印的图像中. 考虑到可逆嵌入阶段对水印能量的影响,Wang等人[17]在haar小波变换域中将原始图像分为2个独立区域,其中,水印嵌入到低频系数区域,而原始区域和水印区域之间的差异嵌入到高频区域. 由于第2阶段是可逆地嵌入差异以恢复原始图像,因此在鲁棒性约束下,第1阶段的水印失真应尽可能小. 现有的2阶段水印框架方法,对那些类似加性噪声的操作有着令人满意的鲁棒性. Ghosh等人[18]选择基于整数的小波变换,以较少的计算时间产生高质量的水印图像,通过选择高频系数进行数据隐藏,进一步保证图像的不可感知性. 但这些方法所利用的鲁棒性特征对几何变形十分敏感. 即使图像受到轻微的几何变形(如旋转或缩放),也往往无法检测到水印. 如何提高对几何攻击的抵抗能力在图像水印领域仍然具有挑战性.

Liang等人[19]通过使用Paillier密码系统为加密图像提出一种鲁棒且可逆的水印方案,使用直方图将水印信息嵌入加密图像中,再用逆运算将被加密的图像还原为原来的图像. Liu等人[20]设计了一种用于水印关系数据库的零失真盲可逆鲁棒方案,对水印在嵌入前进行加密,保证水印信息的安全性. 此外,它还具有出色的抗数据添加、删除和修改攻击的鲁棒性. 虽然上述方案实现了水印的2个特性,但仍需在鲁棒性和不可感知性之间进行取舍达到最佳效果.

已有的基于矩[21]的方法对图像处理操作具有很好的鲁棒性,但在抵抗几何变形时,由于水印图像和原始图像之间的差异太大,无法实现水印的可逆提取. 因此,需要一种新的基于矩的鲁棒可逆水印策略. 目前,

Hu等人[22]设计了一种新的量化方法,该方法只量化矩的整数部分,且只对几何攻击如旋转、缩放和JPEG压缩的效果显著,对于常见攻击,比如对加性噪声和JPEG2000等攻击的鲁棒性有待加强.

在图像中嵌入水印的研究大部分所能抵抗的攻击为加性噪声攻击,如JPEG压缩等,这些研究对几何攻击非常敏感,但水印在旋转缩放后并不能提取出来. 而正交矩的特性是在旋转缩放平移后仍然保持不变,因此将水印嵌入到矩中就可以抵抗几何攻击. 同时,通过Wang等人[17]和Ghosh等人[18]的实验可以发现,相比高频区域,嵌入到低频区域的水印受到噪声攻击的影响更小,也就是说低频区域鲁棒性更好,适合水印的嵌入. 因此,利用图像经过整数小波变换(Integer Wavelet Transformation,IWT)后的低频系数计算伪Zernike矩是可行的.

针对目前的鲁棒可逆水印(Robust Reversible Watermarking,RRW)方案存在的抗攻击能力较差以及嵌入容量不足等问题,本文采用IWT和伪Zernike矩(Pseudo-Zernike Moments,PZMs)来研究鲁棒可逆水印方案存在的问题. 通过IWT在低频区域计算伪Zernike矩,再通过自适应归一化方法对伪Zernike矩进行选择并将水印嵌入其中. IWT和伪Zernike矩的有效结合使方法在对几何和常见攻击时具有很强的抗干扰能力,自适应归一化方法则进一步增强了可逆水印在相同失真下的鲁棒性. 最后通过改进传统的DC-QIM(Quantization Index Modulation with Distortion Compensation),降低了计算误差等补偿信息.

该方案的贡献包括以下3个方面:

(1)将IWT和PZMs相结合,并采用自适应归一化方法,增强相同嵌入失真下的鲁棒性.

(2)设计了一种改进的DC-QIM方法来优化水印的嵌入,显著减少了可逆水印的辅助信息量.

(3)提出了新的RRW方案,在获得良好的不可见性和可逆性的前提下实现高鲁棒性,优于现有技术.

2　预备知识

2.1　数字水印技术

数字水印(Digital Watermarking,DW)是嵌在其他数据(宿主数据)中具有可鉴别性的数字信号或模式,同时不应影响宿主数据的可用性. 其作为一种被深入研究的成熟信息隐藏技术,已被广泛用于多媒体信息的版权保护和完整性认证领域. 数字水印技术主要由水印生成算法、水印嵌入算法和水印提取算法3个部分组成. 数字水印技术用特殊的方法把某些标识信息嵌入到文本数据或多媒体载体中,这样不仅能认证数据的来源或者完整性,而且可以在出现争议时提供相对应的版权证据. 一般情况下,数字水印的嵌入不会对载体的正常使用造成影响,并且水印也不易被发现、篡改或者损坏,具有一定的安全性.

根据其在信息安全应用中的不同,数字水印被分为可逆水印和鲁棒水印. 可逆水印的关键在于它可以保护原始图像免受嵌入水印信息的影响,适合在高保真领域应用,但无法防御各种攻击是它最大的劣势. 而鲁棒水印更侧重于版权保护,当数字产品在网络上遭受各种攻击时,可以提取水印作为版权证明. 另外,针对水印的特点,水印的特性主要包括不可感知性、鲁棒性和脆弱性[23,24].

不可感知性也叫隐蔽性或者不可见性,是指在一般视觉环境下,嵌入到多媒体上的水印必须具备较好的不为人的感知系统所觉察的特性,通常采取峰值信噪比(Peak Signal to Noise Ratio,PSNR)作为评估指标. PSNR反映了嵌入后的图像和原图像之间的相似度,当PSNR数值较大时,表明2个图像之间的相似度较高,水印图像具有较高的视觉质量.

鲁棒性又称稳健性,反映了水印系统抵抗攻击的能力,水印系统对攻击的抵抗能力越高,表示它的鲁棒性能越好. 比特误码率(Bit Error Rate,BER)是用来作为水印检测误码率的一项指标,表示嵌入水印信息的总量中水印提取误码的总量所占的百分比. 从受攻击图像中提取的水印比特误码率越低,说明水印系统的鲁棒性越好.

水印的脆弱性通常用于多媒体内容的完整性认证. 当要保护的载体遭到损坏、篡改和攻击后,可以通过完整性认证知道其内容是否被改变,以及损坏的有关情况,这往往依赖于水印的脆弱性. 已知判断载体是否完整的认证方法主要是通过相关的计算方法对载体内容操作得出一个hash值,再将hash值转换成二进制比特,最后将多位比特作为水印信息嵌入到载体中就可以用于完整性认证. 微小的改变可以导致hash值有很大的变化,因此hash计算用于篡改认证非常合适.

2.2　伪Zernike矩

伪Zernike矩[25~27]是由图像和伪Zernike多项式的内积获得的正交矩,其中伪Zernike多项式是Zernike多项式的变体,其所用的正交多项式集为单位圆上的完备正交集. 除了旋转和缩放不变性外,PZMs比ZMs更稳健,对图像噪声的敏感性更低. 值得注意的是,对于相同的矩阶,PZMs的数量是ZMs的2倍. 由于这些理想的特性,PZMs被广泛用于许多图像处理和模式识别应用.

假设$V_{nm}(x,y)$表示伪Zernike多项式,该多项式是一组完全正交函数,$f(x,y),(x,y\in[1,M])$是一个图像函数. 然后将单位圆上定义的$f(x,y)$分解为$V_{nm}(x,y)$:

$$f(x,y)=\sum_{n=0}^{N}\sum_{m=-n}^{n}\boldsymbol{P}_{nm}V_{nm}(x,y) \tag{1}$$

其中，$\boldsymbol{P}_{nm}$表示具有重复m的n阶PZMs，n为非负整数，m为符合$0\leqslant|m|\leqslant n$的整数．$\boldsymbol{P}_{nm}$是$f(x,y)$和$V_{nm}(x,y)$的内积，即

$$\boldsymbol{P}_{nm}=\frac{n+1}{\pi}\iint_{x^2+y^2\leqslant 1}f(x,y)\,V_{nm}^{*}(x,y)\,\mathrm{d}x\mathrm{d}y \tag{2}$$

其中，$V_{nm}^{*}(x,y)$表示$V_{nm}(x,y)$的共轭．$V_{nm}(x,y)$计算如下：

$$V_{nm}(x,y)=R_{nm}(\rho)\,\mathrm{e}^{\mathrm{j}m\theta} \tag{3}$$

这里，n为非负整数，m为符合$0\leqslant|m|\leqslant n$的整数，$\rho=\sqrt{x^2+y^2}$，$\theta=\tan^{-1}(y/x)$.

径向伪Zernike多项式定义为

$$R_{nm}(\rho)=\sum_{c=0}^{n-|m|}\frac{(2n+1-c)!\,\rho^{n-c}}{c!\,(n+|m|+1-c)!\,(n-|m|-c)!} \tag{4}$$

式(2)适用于连续函数，其离散版本定义为

$$\boldsymbol{P}_{nm}=\frac{n+1}{\pi}\sum_{i=1}^{M}\sum_{j=1}^{M}f(x_i,y_j)V_{nm}^{*}(x_i,y_j)\Delta x\Delta y \tag{5}$$

其中，$x^2+y^2\leqslant 1$，$\Delta x=\Delta y=\frac{2}{M}$，$M\times M$表示图像的大小．

PZMs可用于重建原始函数，即

$$\hat{f}(x,y)=\sum_{n=0}^{N}\sum_{m=-n}^{n}\boldsymbol{P}_{nm}V_{nm}(x,y) \tag{6}$$

其中，$V_{nm}(x,y)$是一组完整的正交函数，当$N\to\infty$，$\hat{f}(x,y)$接近于$f(x,y)$. 在实践中，$\hat{f}(x,y)$并不近似于$f(x,y)$，由于$\boldsymbol{P}_{nm}$和$V_{nm}(x,y)$在数值上都变得不稳定，并且对于高阶矩来说不准确．

PZMs的模有旋转不变的性质，假设极坐标下的原始图像$f(\rho,\theta)$的伪Zernike矩$\boldsymbol{P}_{nm}$与旋转α角度的图像$f^{\mathrm{r}}(\rho,\theta)$的伪Zernike矩$\boldsymbol{P}_{nm}^{\mathrm{r}}$关系为

$$\boldsymbol{P}_{nm}^{\mathrm{r}}=\boldsymbol{P}_{nm}\mathrm{e}^{-\mathrm{j}m\alpha} \tag{7}$$

由于PZMs是复数矩，一般使用PZMs的模来体现它的旋转不变性．但此时不具备平移和缩放不变性，需要对目标进行归一化间接使PZMs达到平移和缩放不变．在文献[28]中引入了归一化操作，作者提出利用零阶矩对Zernike矩进行归一化．归一化后，Zernike矩的振幅保持旋转和缩放不变，这同样适用于伪Zernike矩．

2.3 整数小波变换

IWT[18]是DWT的演变，适用于在可逆水印中使用整数像素．在以往的工作中[10]，图像的DWT低频系数在受到噪声攻击后的值变化不大，DWT变换对不同强度的噪声有很好的抵抗力．IWT继承了DWT的优点，实现了真正的可逆性，其低复杂度实现了图像的完全无损压缩，为可逆水印的实现提供帮助．

3 采用IWT和自适应伪Zernike矩的鲁棒可逆水印方案

本文提出一种采用IWT和自适应伪Zernike矩的鲁棒可逆水印方案，该方案使用了IWT计算、PZMs的自适应归一化方法、优化的嵌入策略．另外，还包括完整性认证、水印的提取和原始图像的恢复．

3.1 水印嵌入

水印嵌入分别将鲁棒水印和辅助信息嵌入到载体图像中．图1展示了本文水印和辅助信息的嵌入过程．在鲁棒水印嵌入阶段，首先由图像进行一级IWT得到的低频区域计算PZMs，然后通过自适应归一化方法和优化的嵌入策略选择符合条件的PZMs并对其嵌入水印，接着对水印图像重构得到中间水印图像It，经过逆小波变换得到水印图像Iw，并对过程中产生的量化误差和取整误差进行保留．在可逆嵌入阶段，将生成的量化误差、取整误差和由水印图像计算得到的hash值合并成辅助信息，可逆嵌入到水印图像中生成可逆水印图像Iw1.

（1）计算PZMs

假设大小为$M\times M$的Img是给定图像，Ic经过IWT的低频区域，$\boldsymbol{P}_{nm}$是阶数为n和重复数为$m\left(0\leqslant n\leqslant N,0\leqslant|m|\leqslant n\right)$的PZMs，$N$表示最大阶数．计算原始图像Img低频区域内切圆的径向伪Zernike多项式R_{nm}，计算相应的伪Zernike矩$\boldsymbol{P}_{nm}$.

尽管$\boldsymbol{P}_{nm}$可用于计算离散数字图像，但其仍存在几何和积分近似误差[29,30]．由于这些误差，Xin等人[31]证明了$m=4j(j\in Z)$的伪Zernike矩偏离正交性，无法准确计算．则$m=4j$的PZMs不能用于水印嵌入，合格的伪Zernike矩被选择为$\boldsymbol{C}=\{\boldsymbol{P}_{nm},0<n\leqslant N,0<m\leqslant n,m\neq 4j\}$.

假设一个选定的伪Zernike矩嵌入一个水印位，并且总共有L个($L<\boldsymbol{C}$的长度)水印比特$w_i\in\{0,1\}$．然后，通过密钥key从$\boldsymbol{C}$中随机选择L个伪Zernike矩，其产生$\boldsymbol{P}=\{\boldsymbol{P}_{n1,m1},\boldsymbol{P}_{n2,m2},\cdots,\boldsymbol{P}_{nL,mL}\}$.

（2）自适应归一化

由于缩放操作会改变PZMs的值，通常采用归一化策略来解决[31].

$$\boldsymbol{P}_{ni,mi}^{\mathrm{R}}=\frac{\boldsymbol{P}_{ni,mi}}{\boldsymbol{P}_{00}} \tag{8}$$

通过归一化，$\boldsymbol{P}_{ni,mi}^{\mathrm{R}}$面对缩放操作保持不变．由于低阶PZMs通常比高阶PZMs对信号处理更具鲁棒性，因此高阶PZMs应具有比低阶PZMs更大的嵌入强度，使相同嵌入失真的情况下鲁棒性最大．鉴于此，采用一种自适应归一化方法：

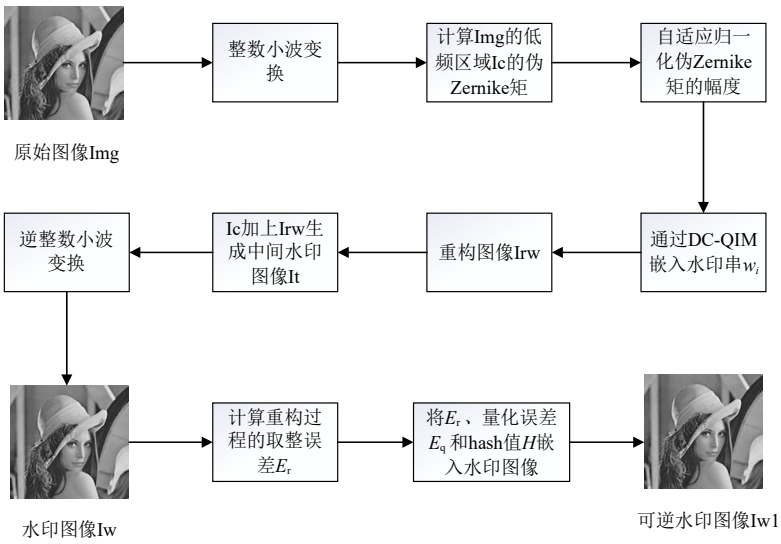


图1　发送端水印嵌入流程

$$\boldsymbol{P}_{ni,mi}^{\mathrm{R}}=\frac{\boldsymbol{P}_{ni,mi}}{\boldsymbol{P}_{00}}\times T_i \tag{9}$$

其中,T_i是大于0并且相对于PZMs阶变化的自适应归一化权重,$\boldsymbol{P}_{ni,mi}^{\mathrm{R}}$在$[0,T_i]$的范围内.

由于理论上很难推导出最佳T_i,在研究工作中,T_i设为

$$T_i=T_{\mathrm{s}}+\alpha\times n_i \tag{10}$$

其中,T_{s}表示自适应权重的起始值,$\alpha(\alpha>0)$是调整嵌入水印强度的归一化权重,n_i是与水印比特w_i对应的PZMs阶数. 参数T_{s}和α用于控制水印图像的不可见性,通过实验模拟来实际确定.

如上所述,归一化的伪Zernike矩$\boldsymbol{P}_{ni,mi}^{\mathrm{R}}$对缩放是不变的. 一直PZMs的幅度具有旋转不变的特性,将幅度$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|$作为水印的载体. 可以实现旋转和缩放不变性. $\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|$作为水印载体,可以采用带抖动补偿的量化索引调制技术(DC-QIM)来嵌入水印比特w_i,其表示为

$$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}j}\right|=\left\lfloor\left(\left\lfloor\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|\right\rfloor/\Delta\right\rfloor\times\Delta+\lambda_i(j),\ i=1,2,\cdots,L,\ j\in\{0,1\} \tag{11}$$

其中,$\lambda_i(j)$是具有$\lambda_i(1)=\lambda_i(0)+\Delta/2$约束的抖动值,$\lfloor\cdot\rfloor$是向下取整函数,$\Delta$是量化步长.

通过DC-QIM,$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R0}}\right|$和$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R1}}\right|$代表载体$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|$嵌入0和1的水印版本. 由于归一化PZMs是实数,所以量化误差也是实数. 由于要实现原始图像的可逆性,必须要保存这些实数,用大量的比特来保存. 针对这个问题,通过取整量化误差优化传统的DC-QIM. 量化误差$E_{\mathrm{q}}=\left\{E_{\mathrm{q}i}=\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}j}\right|-\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|,i=1,2,\cdots,L,j\in\{0,1\}\right\}$,具体来说,第1轮对$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|$取接近的整数,也就是变成$\left\lfloor\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|\right\rfloor$,并且计算$D_i=\left|\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|-\left\lfloor\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|\right\rfloor\right|$,改进传统的DC-QIM,即

$$\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}j}\right|=\left\lfloor\left(\left\lfloor\left\lfloor\left|\boldsymbol{P}_{ni,mi}^{\mathrm{R}}\right|\right\rfloor-\lambda_i(j)\right)/\Delta\right\rfloor\times\Delta+\lambda_i(j)-D_i \tag{12}$$

其中,$[\cdot]$是四舍五入函数,通过式(12)计算的量化误差将是整数,用更少的比特来保存. 与传统嵌入方法不同的是,在式(12)中采用舍入函数来代替式(11)中的取整函数,进一步减少量化误差.

本方案采用了PZMs自适应归一化方法,对低阶PZMs采用权重化策略,即使用T_{s}和归一化权重α,在相似PSNR的情况下比较它们对旋转、缩放、JPEG、JPEG2000、高斯白噪声和椒盐噪声攻击的鲁棒性性能,部分实验结果如表1所示. 在实验模拟中,T_i根据式(10)确定,随着图像变化. 通过大量实验得出,T_{s}为1 900,α为10时,鲁棒性较好.

表1　不同参数下对不同攻击的鲁棒性性能

单位:%(平均BER)

T_{s}	α	旋转	缩放	JPEG	JPEG2000	高斯	椒盐
2 000	8	0	0.59	0.08	0.31	3.25	0.36
2 000	10	0	0.44	0	0.62	2.95	0.18
2 000	12	0	0.49	0	0.08	2.76	0.24
2 000	14	0	0.59	0.08	0.93	2.76	0.18
1 900	**10**	**0**	**0.54**	**0**	**0.16**	**2.70**	**0.18**
2 100	10	0	0.63	0.08	0.16	3.55	0.54

注:加黑数据鲁棒性最好.

(3)鲁棒水印图像重构

在生成带水印的归一化PZMs之后,进行逆归一化以产生带水印的PZMs,即

$$\boldsymbol{P}^{\mathrm{w}}_{ni,mi}=\frac{\left|\boldsymbol{P}^{\mathrm{Rw}}_{ni,mi}\right|}{\left|\boldsymbol{P}^{\mathrm{R}}_{ni,mi}\right|}\times\boldsymbol{P}^{\mathrm{R}}_{ni,mi} \tag{13}$$

在获得带水印的$\boldsymbol{P}^{\mathrm{w}}_{ni,mi}$之后，继续从$\boldsymbol{P}^{\mathrm{w}}_{ni,mi}$重建鲁棒水印图像. 为了保证重建图像的像素值为真实值，首先对$\boldsymbol{P}_{ni,mi}$的共轭(即$\boldsymbol{P}^{\mathrm{w}}_{ni,-mi}$)应用与$\boldsymbol{P}_{ni,mi}$相同的嵌入操作，然后如式(14)重构中间水印图像It：

$$\mathrm{It}=\mathrm{Ic}+\left\{\begin{array}{l}\sum\limits_{i=1}^{L}\left[(\boldsymbol{P}^{\mathrm{w}}_{ni,mi}-\boldsymbol{P}_{ni,mi})V_{ni,mi}\right.\\ \left.+(\boldsymbol{P}^{\mathrm{w}}_{ni,-mi}-\boldsymbol{P}_{ni,-mi})V_{ni,-mi}\right]\end{array}\right\} \tag{14}$$

最后使用逆IWT将中间水印图像还原原始图像尺寸变成水印图像：

$$\mathrm{Iw}=\mathrm{RIWT}(\mathrm{It}) \tag{15}$$

(4)可逆嵌入辅助信息

原始图像由于鲁棒水印嵌入导致失真. 为确保在没有攻击情况下的可逆性，需要将引起的失真保存在Iw中. 为此，通常采用可逆水印技术，形成了可逆嵌入阶段. 在可逆嵌入阶段，首先使用Iw的低频区域计算PZMs，结合量化误差生成与重构水印图像近似的去除水印图像，构建辅助信息并将其嵌入Iw中，生成具有鲁棒性的可逆水印图像Iw1.

如上所述，改进的DC-QIM被设计用于嵌入鲁棒水印. 由于嵌入水印方法的量化操作会导致幅度存在变化. 为确保可逆性，需要保存量化误差E_{q}. 由于PZMs重构图像中存在舍入误差E_{r}，按照Hu等人[22]提出的方法计算，由Img和Iw之差计算得出. 因此，E_{r}也构成辅助信息的一部分. 对于攻击认证，进一步考虑了辅助信息的另一部分. 在没有攻击的情况下，需要恢复鲁棒水印和原始图像，而在攻击场景中，只提取鲁棒水印. 因此，当接收到带水印的图像时，首先需要检查收到的图像是否受到攻击. 为此，采用了哈希技术，也就是说，对嵌入了水印和辅助信息的图像进行hash操作，并产生hash值H.

总之，该方案中的辅助信息由E_{q}、E_{r}和H组成. 在构造辅助信息之后，将其可逆嵌入到水印图像Iw中. 由于辅助信息的大大减少以及在低频区域中计算矩，则直接将辅助信息嵌入到载体图像像素中并不会产生太大的影响，接着生成了同时具有水印和辅助信息的可逆水印图像Iw1. 由于空间限制，可逆嵌入的细节建议参考文献[32].

3.2 完整性认证

如图2所示，在接收端收到传输图像Iw2后，首先进行完整性认证，检查图像是否受到攻击. 具体来说，首先对提取出辅助信息后的图像计算完整性认证哈希序列$H1$. 再与提取的哈希值H进行比较，如果H完全等于$H1$，认为接收到的图像没有受到攻击，否则，传输图像遭到了无意或故意攻击.

3.3 提取水印与恢复图像

完整性认证完成后，接收端可以判断接收到的图像是否受到攻击. 如果接收到的图像没有受到攻击，则可以正确提取认证水印，并完全恢复原始图像. 首先，应用文献[32]中的方法从Iw2中提取辅助信息，其中，辅助信息包含E_{q}、E_{r}和H. 并且恢复去除了辅助信息的图像，得到鲁棒水印图像I′w. 在不受攻击的情况下，它实际上等价于嵌入端的鲁棒水印图像Iw. 然后再从I′w中提取鲁棒水印，对I′w计算PZMs，采用由秘密信道发送的与嵌入端相同密钥key，从所有PZMs中选择相同的矩$\boldsymbol{P}^{\mathrm{rw}}_{ni,mi}$，继而利用式(9)得到$\boldsymbol{P}^{\mathrm{Rrw}}_{ni,mi}$，再通过式(16)和式(17)计算鲁棒水印：

$$\left|\boldsymbol{P}^{\mathrm{Rr}j}_{ni,mi}\right|=\left[\left(\left(\left\lfloor\left|\boldsymbol{P}^{\mathrm{Rrw}}_{ni,mi}\right|\right\rfloor-\lambda_i(j)\right)\Big/\Delta\right\rceil\times\Delta+\lambda_i(j),\right. \tag{16}$$

$$\left.i=1,2,\cdots,L,\ j\in\{0,1\}\right.$$

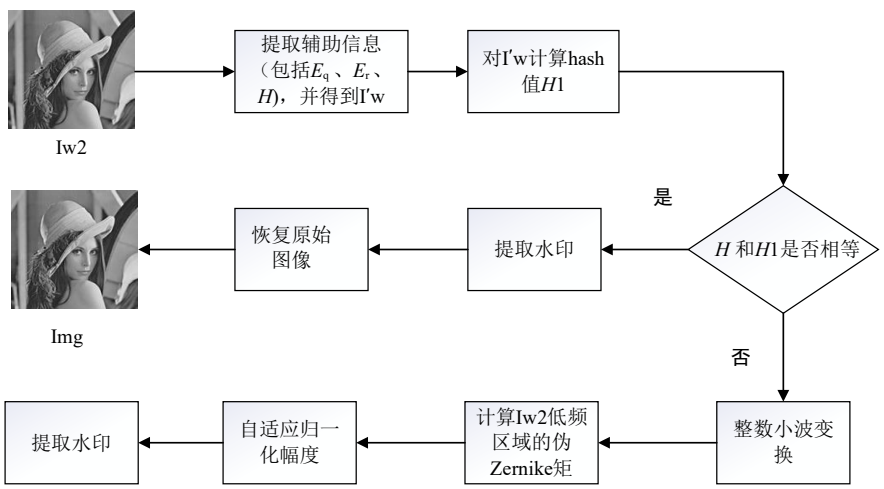


图2 接收端水印提取流程

$$w_i=\begin{cases}0, \text{ if } \left|\boldsymbol{P}_{ni,mi}^{\text{Rrw}}\right|-\left|\boldsymbol{P}_{ni,mi}^{\text{Rr0}}\right| \leqslant \left|\boldsymbol{P}_{ni,mi}^{\text{Rrw}}\right|-\left|\boldsymbol{P}_{ni,mi}^{\text{Rr1}}\right| \\ 1, \text{ if } \left|\boldsymbol{P}_{ni,mi}^{\text{Rrw}}\right|-\left|\boldsymbol{P}_{ni,mi}^{\text{Rr0}}\right| > \left|\boldsymbol{P}_{ni,mi}^{\text{Rrw}}\right|-\left|\boldsymbol{P}_{ni,mi}^{\text{Rr1}}\right|\end{cases} \tag{17}$$

$$\left|\boldsymbol{P}_{ni,mi}^{\text{Rr}}\right|=\left|\boldsymbol{P}_{ni,mi}^{\text{Rrw}}\right|-E_{\text{q}i} \tag{18}$$

$$\boldsymbol{P}_{ni,mi}^{\text{r}}=\frac{\left|\boldsymbol{P}_{ni,mi}^{\text{Rr}}\right|}{\left|\boldsymbol{P}_{ni,mi}^{\text{Rrw}}\right|}\times\boldsymbol{P}_{ni,mi}^{\text{rw}} \tag{19}$$

最后,通过式(18)和式(19)计算得到$\boldsymbol{P}_{ni,mi}^{\text{r}}$,进行重构恢复,得到去除水印的图像IW. 因此,通过进一步添加提取的舍入误差E_{r},原始图像可以恢复为

$$I=\text{IW}+E_{\text{r}} \tag{20}$$

这里,I和原始图像Img是完全一样的.

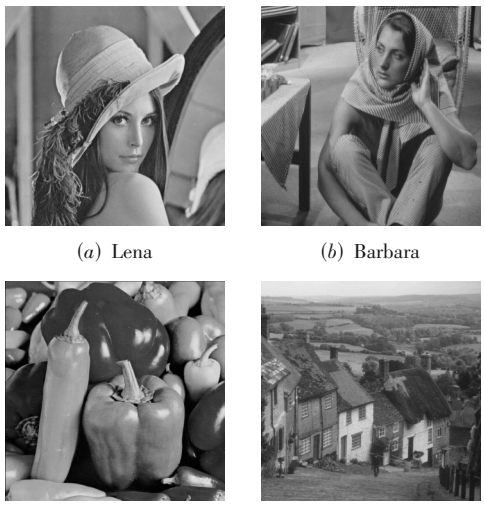
本文对辅助信息的可逆嵌入和提取方法是采用文献[32]的可逆嵌入算法. 根据文献[32]所述,如果Iw2受到攻击,图像的像素值会发生改变,这会导致用于恢复图像的辅助信息(E_{q}、E_{r}和H)无法被正确提取,因而原始图像无法完全恢复. 在这种情况下,可以直接使用Iw2来生成PZMs进行提取鲁棒水印.

4　实验结果及分析

本文实验对象为从http://dde.bing-hamton.edu下载的BOSSbase_1.01数据集,其中4张灰度图像的实验结果被详细列出,同时也对数据集做了比较测试. 本方案主要涉及5个参数,即自适应权重T_{s}、调整嵌入水印强度的归一化权重α、PZMs的最大阶数N、嵌入水印比特w_i的数量L和量化嵌入水印的步长Δ. 因为要平衡水印的鲁棒性和不可感知性,对于T_{s}、α和Δ,它们分别被设置为T_{s}=1 900、α=10和Δ=32作为实际可行的参数,这样平均PSNR约为39 dB. 为了方便容量说明和性能比较,L分别被设置成2种容量大小,即L=128和L=256. 通过权衡PZMs数量和计算复杂性,分别对L=128和L=256的阶数设置N=18和N=26.

在数据集BOSSbase_1.01上做了无攻击情况下的水印提取和图像恢复实验. 实验结果得到接收端接收并提取水印的BER为0,恢复后的图像和原始图像的PSNR为∞,SSIM=1. 这表明本文方案在无攻击情况下具有可逆性,接收端可以正确提取水印并完全恢复原始图像.

本文和6个最先进的方案(Wang[17]、Liu[20]、Xiang[22]、Wang[33]和Sun[34](SURF和ORB))进行对比,在128 bits和256 bits鲁棒水印的情况下,这里使用了4幅典型灰度图像进行展示说明,包括Lena、Barbara、Peppers和Goldhill,如图3所示. 为了公平比较,将与同一原始测试图像相对应的不同方案水印图像的PSNR调整为基本相同.



(a) Lena　(b) Barbara　(c) Peppers　(d) Goldhill

图3　4幅典型灰度图像

4.1　不可感知性分析

表2总结了测试图像的水印图像和可逆水印图像在不同嵌入容量时的PSNR. 表3对比了不同方案在128 bits下Iw1的PSNR值. 可以看出在嵌入128 bits时,本方案中的可逆水印图像的PSNR基本在39 dB以上,这表明图像的不可见性达到了良好水平. 同时,即使是在嵌入256 bits时,PSNR的变化幅度也非常小,保持在38 dB以上. 从4幅图像的PSNR平均值来看,本方案的PSNR值仅略低于Xiang的方案,高于其他4种方案,后续的鲁棒性比较实验具有说服力. 表4对比了2种不同方案所需的辅助信息量. 可以看出,本文方案提出的方法减少了嵌入水印所需的辅助信息量大小,更好地满足了水印的不可感知性. 以当前的PSNR设置,接下来可以公平地评估针对常见攻击和几何变换的鲁棒性性能.

表2　Iw和Iw1在嵌入不同水印比特时的PSNR

图像名称	128 bits		256 bits	
	Iw	Iw1	Iw	Iw1
Lena	39.05	39.01	39.48	38.68
Goldhill	40.26	40.19	40.26	38.02
Barbara	40.47	40.41	39.89	38.77
Peppers	39.62	39.38	39.65	38.61

表3　128 bits嵌入容量下不同方案的Iw1的PSNR的对比

图像名称	不同方案的PSNR/dB					
	Wang[17]	Liu[20]	Wang[33]	Sun[34]	Xiang[22]	Proposed
Lena	38.85	38.47	37.94	37.63	39.44	39.01
Goldhill	38.59	38.89	38.22	38.88	40.17	40.19
Barbara	39.00	37.85	38.05	38.94	39.24	40.41
Peppers	38.23	38.08	39.84	37.94	40.76	39.38
Average	38.67	38.32	38.51	38.35	39.90	39.75

表4 不同方法所需辅助信息的对比实验 单位:bits

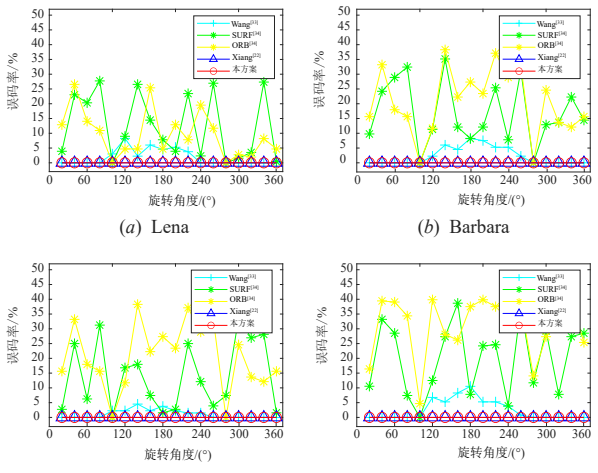
方案	Lena	Barbara	Peppers	Goldhill
本文方案	8 360	11 184	6 248	9 488
固定归一化权值和无IWT	39 256	39 728	49 560	16 184

4.2 鲁棒性分析

本节对几何攻击(包括旋转和缩放)和常见攻击(包括JPEG压缩、JPEG2000、高斯白噪声和椒盐噪声)进行鲁棒性性能分析. 由于Liu和Wang[17]的鲁棒可逆水印方法不能抵抗几何变形,本方案主要与Xiang、Wang[33]和Sun提出的方案进行几何攻击比较,而常见攻击测试与其他4种方案都进行比较. 实验结果分别展示了在128 bits和256 bits下不同方案对不同攻击的鲁棒性性能.

4.2.1 128 bits的比较

图4清晰地表明,当嵌入128 bits时,对于任何旋转角度,本方案和Xiang方案的BER值均为0,优于Wang[33]和Sun的方案. 这表明PZMs和ZMs都能很好地抵抗旋转攻击. 如图5所示,本方案相比Xiang的方案在缩放因子大于0.6时,面对缩放攻击具有更好的鲁棒性性能,且BER能够一直保持较低水平,但比Wang[33]的方案略差. Wang[33]的方案能保持较低的BER,这主要归功于特征的提取算法,选择以提取的特征点为中心的几个大小不一的非重叠局部圆形区域作为水印嵌入区域. 但这同时也影响了该方案在旋转等噪声方面的鲁棒性.

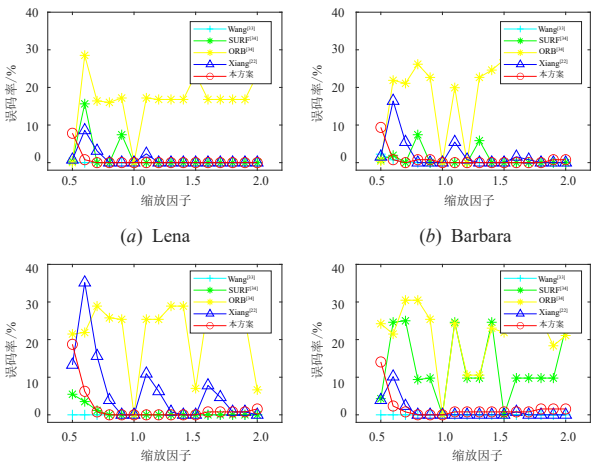


(a) Lena (b) Barbara

(c) Peppers (d) Goldhill

图4 不同方案在128 bits嵌入容量下对旋转攻击的鲁棒性

图6展示了各自的方案能很好地抵抗JPEG压缩,对于任何压缩质量因子,本方案的BER都为0,而其他对比方案的BER都有不为0情况存在,这表明本方案对所有质量因子的JPEG压缩都拥有非常好的鲁棒性性能. 这是因为本方案所采用的低阶矩具有抵抗压缩

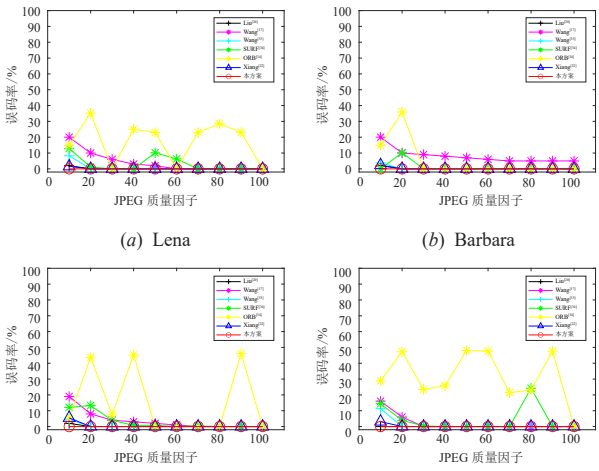


(a) Lena (b) Barbara

(c) Peppers (d) Goldhill

图5 不同方案在128 bits嵌入容量下对缩放攻击的鲁棒性

攻击的特性. 从图7可以看出,本方案对JPEG2000压缩的BER在不同压缩比下变化的幅度非常小,实验结果证明本方案比其他方案具有更好的性能. 同时,即使当压缩比为100时,本方案在BER方面也极具竞争力. 这表明提出的自适应归一化策略以及IWT的有效性.

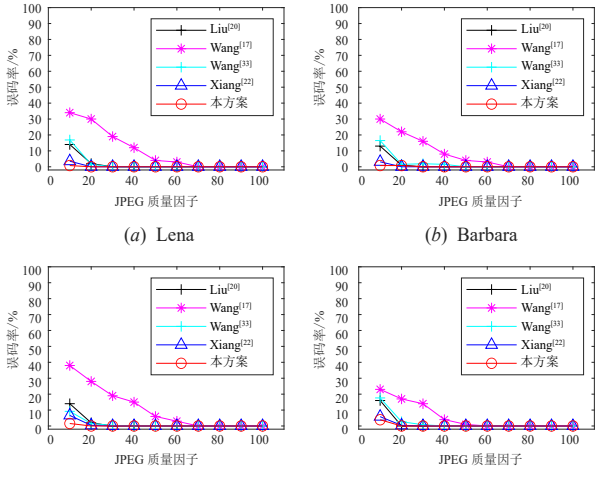


(a) Lena (b) Barbara

(c) Peppers (d) Goldhill

图6 不同方案在128 bits嵌入容量下对JPEG压缩的鲁棒性

由图8可知,除Peppers图像之外的其他图像,本方案的BER都优于Liu的方案,主要是本方案对高斯白噪声具有高度鲁棒性的低阶PZMs中量化嵌入了水印. 而Liu的方案主要是在空间域的中频子带里嵌入了水印信息,所以他的方案在高斯白噪声的鲁棒性性能方面比将水印嵌入到矩中的方案更差. 此外,本方案的BER略高于Wang[17]的方案. 这是因为Wang[17]将鲁棒水印嵌入到比低阶PZMs和ZMs具有更高鲁棒性的haar变换的低频子带中. 虽然本方案也使用了低频区域计算PZMs来嵌入水印,但是由于Wang[17]是直接将水印嵌

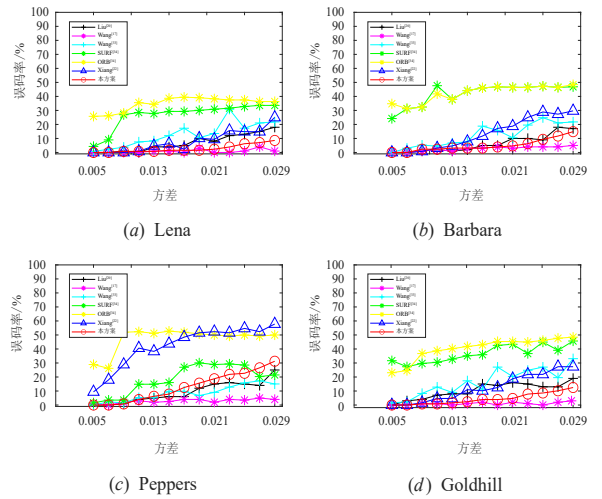


(*a*) Lena　(*b*) Barbara

(*c*) Peppers　(*d*) Goldhill

图7　不同方案在128 bits嵌入容量下对JPEG2000的鲁棒性

入低频子带,所以在抵抗高斯白噪声的效果上要优于本方案,但是Wang[17]的方案仍不能抵抗几何变换. 另外,本方案总体上略好于Xiang的方案,这归因于PZMs对图像噪声的敏感性低于ZMs.



(*a*) Lena　(*b*) Barbara

(*c*) Peppers　(*d*) Goldhill

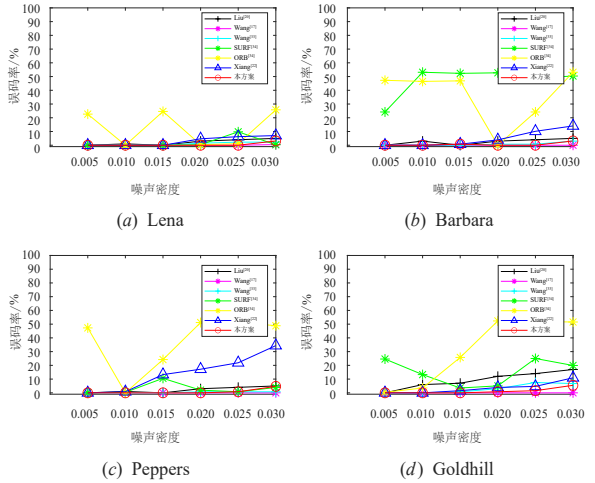
图8　不同方案在128 bits嵌入容量下对高斯白噪声的鲁棒性

如图9所示,本方案在各种噪声密度时的BER均低于5%,仅略高于Wang[17]的方案,这再次表明PZMs在抵抗椒盐噪声时具有较好的鲁棒性.

如表5所示,在数据集BOSSbase_1.01上与Xiang和Wang[33]的方案做了对比实验,明显看出,在嵌入128 bits水印下,本文方案在数据集中的鲁棒性性能仅在缩放噪声下略差于Wang[33]的方案. 综合来看,相比Xiang和Wang[33]的方案,本文方案在128 bits嵌入容量的鲁棒性性能是最优的.

4.2.2　256 bits的比较

在该模拟中,测试图像被嵌入了相同的256 bits水印信息. 与嵌入128 bits水印的情况类似,通过对嵌入256 bits的水印图像进行旋转、缩放、高斯白噪声、椒盐噪声、JPEG、JPEG2000攻击,并用实验仿真测试所提取的水印比特的BER.



(*a*) Lena　(*b*) Barbara

(*c*) Peppers　(*d*) Goldhill

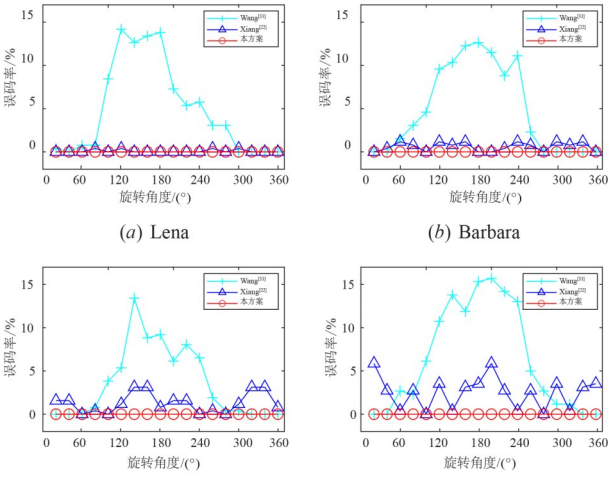
图9　不同方案在128 bits嵌入容量下对椒盐噪声的鲁棒性

表5　128 bits嵌入容量下不同方案对不同攻击的鲁棒性性能数据集测试　　单位:%(平均BER)

方案	旋转	缩放	JPEG	JPEG2000	高斯	椒盐
本文	0	1.17	0	0.60	6.20	0.50
Xiang	0	2.06	0.25	3.67	15.59	4.38
Wang[33]	1.95	0.05	0.70	10.73	12.52	1.28

从图10可知,Xiang和Wang[33]的方案对旋转攻击在嵌入256 bits时的BER与嵌入128 bits相比有所升高,但本方案的BER依旧为0. 结合图4可知,本方案在嵌入128 bits和256 bits时,对旋转攻击的鲁棒性都十分优越.

图11和图5的对比表明,对于某些特定的缩放因子,3种的方案的鲁棒性显著降低且总体看来BER的变

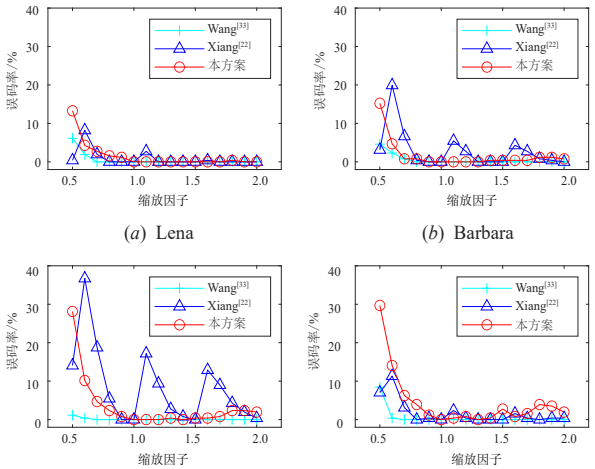


(*a*) Lena　(*b*) Barbara

(*c*) Peppers　(*d*) Goldhill

图10　不同方案在256 bits嵌入容量下对旋转攻击的鲁棒性

化幅度较大，而本方案的BER相比Xiang总体呈下降趋势．和图5一样，Wang[33]的方案选择几个以特征点为圆心的特征区域来嵌入水印，对缩放噪声的鲁棒性较强．



(*a*) Lena (*b*) Barbara

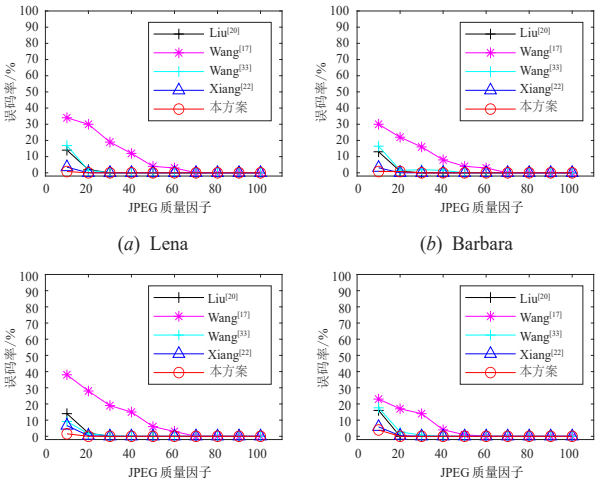
(*c*) Peppers (*d*) Goldhill

图11 不同方案在256 bits嵌入容量下对缩放攻击的鲁棒性

无论是图6还是图12，两者都显示在对比JPEG压缩的性能时，本方案和Xiang的方案都表现出了对JPEG压缩更好的鲁棒性．同时Liu和Wang[33]的方案在当压缩因子大于20时，BER结果也都很低．但是在质量因子为10时，Liu、Wang[17]和Wang[33]的方案的BER值过高，Wang[17]的方案的BER甚至超过20%，这表明对比方案此时的鲁棒性最差．除此之外，与图6相比，相较于嵌入128 bits的情况，在嵌入的水印比特数加倍的情况下，本方案和Xiang方案的BER在质量因子为10时也只是略微升高．图7和图13共同反映了在不同的嵌入容量下，对于JPEG2000攻击，本方案在任何的压缩比下都表现出了比其他方案更好的鲁棒性，这意味着本方案中的自适应归一化和IWT方法提升了水印的鲁棒性．

由图14和图8的比较可以得出，在图像中嵌入256 bits水印时的抗高斯白噪声的性能与嵌入128 bits时相似．其主要区别是Xiang的方案在嵌入256 bits情况下的鲁棒性明显下降，而本方案的鲁棒性能仍保持一个较好水平．这种情况出现的主要原因是在相同阶数的条件下，ZMs的数量小于PZMs的数量，则Xiang的方案需要更多高阶数的ZMs来承载更大容量的水印比特，其鲁棒性大大降低．此外，水印容量越大，用于还原原始图像的辅助信息数量就越多，那么辅助信息在水印区域中所占的像素就会越多，进一步降低了水印的鲁棒性．

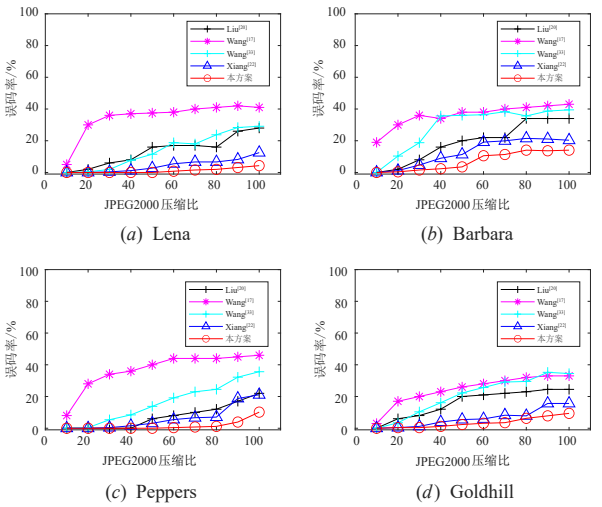
图15和图9显示，除Wang[17]的方案外，本方案和其



(*a*) Lena (*b*) Barbara

(*c*) Peppers (*d*) Goldhill

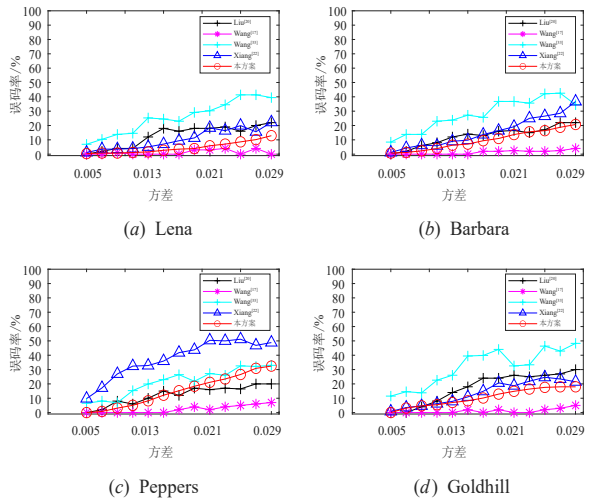
图12 不同方案在256 bits嵌入容量下对JPEG压缩的鲁棒性



(*a*) Lena (*b*) Barbara

(*c*) Peppers (*d*) Goldhill

图13 不同方案在256 bits嵌入容量下对JPEG2000的鲁棒性

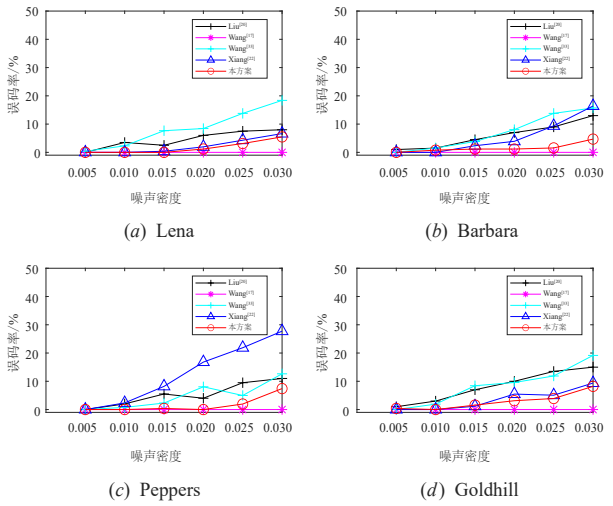


(*a*) Lena (*b*) Barbara

(*c*) Peppers (*d*) Goldhill

图14 不同方案在256 bits嵌入容量下对高斯白噪声的鲁棒性

他方案的鲁棒性能都在一定程度上减弱,具体原因在对128 bits的实验分析中已经探讨过. 这意味着设计方案中将原图通过IWT得到的低频区域用于计算PZMs、使用自适应归一化和改进的DC-QIM量化嵌入方法都在一定程度上仍对不同攻击具有更加优秀的鲁棒性.



(*a*) Lena　(*b*) Barbara

(*c*) Peppers　(*d*) Goldhill

图15　不同方案在256 bits嵌入容量下对椒盐噪声的鲁棒性

如表6所示,在数据集BOSSbase_1.01上与Xiang和Wang[33]的方案做了对比实验. 很明显可以看出,在嵌入256 bits水印下,本文方案在数据集中的鲁棒性性能仅在缩放噪声下略差于Wang[33]的方案. 综合来看,相比Xiang和Wang[33]的方案,本文方案在256 bits嵌入容量的鲁棒性性能是最优的.

表6　在256 bits嵌入容量下不同方案对不同攻击的鲁棒性性能数据集测试　　单位:%(平均BER)

方案	旋转	缩放	JPEG	JPEG2000	高斯	椒盐
本文	0	2.74	0.20	3.35	9.85	1.92
Xiang	1.12	3.45	2.04	7.50	19.37	5.97
Wang[33]	4.96	0.41	1.80	19.93	26.78	7.23

4.3　消融实验

本节为了进一步通过实验来证明自适应归一化方法的有效性,做了相关的消融实验,在PSNR接近的情况下对比2种方案的鲁棒性性能.

如表7所示,本文的方案在高斯噪声、椒盐噪声、缩放、旋转、JPEG以及JPEG2000攻击下的平均BER都低于固定的归一化方法. 由此可以证明自适应归一化方法能够提升图像水印的鲁棒性.

表7　在IWT下自适应归一化与固定归一化方案对不同攻击的鲁棒性性能比较　　单位:%(平均BER)

方案	高斯	椒盐	缩放	旋转	JPEG	JPEG2000
自适应归一化	6.20	0.50	1.17	0	0	0.60
固定归一化	7.74	1.17	1.38	0	0.04	0.82

4.4　时间复杂度

本方案、Xiang的方案和Wang[33]的方案都利用矩进行水印嵌入,其时间复杂度都是$O(n^2)$. 本方案在计算矩之前对图像进行了IWT处理,这会导致一定的时间成本. 同时,由于只计算图像低频域的矩,而低频域图像只有原图像的1/4,因此计算矩的时间大大减少. 同时在整个运行时间内,计算矩的时间占比远大于IWT变换耗时,从而本方案总的运行时间少于Xiang和Wang[33]方案的运行时间,实验结果证明了这个结论. 在同一台设备上,本方案的平均运行时间为20 s,Xiang的方案的平均运行时间为62 s,Wang[33]的方案的平均运行时间为92 s.

5　结论

本文提出了一种采用IWT和自适应伪Zernike矩的鲁棒可逆水印方案,该方案通过PZMs和IWT相结合的方法,对低频区域计算PZMs并将水印嵌入其中,提高图像水印对几何和常见攻击时的抗干扰能力;再通过自适应归一化方法对PZMs进行选择,进一步增强了可逆水印在相同失真下的鲁棒性. 通过将量化误差取整的方法改进传统的DC-QIM技术,补偿了舍入误差,显著减少了辅助信息量,增大水印的嵌入容量. 实验模拟表明,本方案对常见攻击和几何攻击都有很高的鲁棒性. 与现有方案相比,本方案在不同攻击的鲁棒性方面都获得了显著提升.

在未来工作中,如何选择更具鲁棒性的PZMs成为一个有趣的话题. 一个伪Zernike矩被用作一个水印比特的载体,随后的研究可以探究如何引入拼接算法实现嵌入一个水印比特到多个伪Zernike矩中以提高鲁棒性. 此外,本文的研究工作涉及的几何变形主要是全局变换,在未来的研究中需要对局部几何变形的鲁棒可逆水印方案加强研究.

参考文献

[1] BOLLA V R, AMANCHA S, GOPAL T V. A two phase copyright protection scheme for digital images using visual cryptography and sampling methods[C]//2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). Piscataway: IEEE, 2016: 2041-2046.

[2] SINGH A K, KUMAR C. Encryption-then-compression-based copyright protection scheme for E-governance[J]. IT Professional, 2020, 22(2): 45-52.

[3] 欧博, 殷赵霞, 项世军. 明文图像可逆信息隐藏综述[J]. 中国图象图形学报, 2022, 27(1): 111-124.
OU B, YIN Z X, XIANG S J. Overview of reversible data

hiding in plaintext image[J]. Journal of Image and Graphics, 2022, 27(1): 111-124. (in Chinese)

[4] LIU S, LIU Y X, WANG Z P, et al. Privacy protection oriented video data hiding method[C]//2019 IEEE 5th Intl Conference on Big Data Security on Cloud, IEEE Intl Conference on High Performance and Smart Computing (HPSC) and IEEE Intl Conference on Intelligent Data and Security. Piscataway: IEEE, 2019: 90-95.

[5] 高光勇, 周正源. 采用可逆信息隐藏技术的高性能彩色图像对比度增强算法[J]. 计算机辅助设计与图形学学报, 2023, 35(7): 1052-1063.
GAO G Y, ZHOU Z Y. High performance color image contrast enhancement algorithm using reversible data hiding[J]. Journal of Computer-Aided Design & Computer Graphics, 2023, 35(7): 1052-1063. (in Chinese)

[6] KUMAR R, JUNG K H. Robust reversible data hiding scheme based on two-layer embedding strategy[J]. Information Sciences, 2020, 512: 96-107.

[7] 高鹏, 柴鹏翔, 郎俊. 基于0-1背包算法的社交网络行为隐写术[J]. 电子学报, 2022, 50(3): 753-758.
GAO P, CHAI P X, LANG J. Behavior steganography in social networks based on 0-1 knapsack algorithm[J]. Acta Electronica Sinica, 2022, 50(3): 753-758. (in Chinese)

[8] 项世军, 杨乐. 基于同态加密系统的图像鲁棒可逆水印算法[J]. 软件学报, 2018, 29(4): 957-972.
XIANG S J, YANG L. Robust and reversible image watermarking algorithm in homomorphic encrypted domain[J]. Journal of Software, 2018, 29(4): 957-972. (in Chinese)

[9] 肖俊, 王颖. 基于多级离散余弦变换的鲁棒数字水印算法[J]. 计算机学报, 2009, 32(5): 1055-1061.
XIAO J, WANG Y. A robust digital watermarking algorithm based on multiple-level discrete cosine transform[J]. Chinese Journal of Computers, 2009, 32(5): 1055-1061. (in Chinese)

[10] WANG S, ZHENG D, ZHAO J Y, et al. Adaptive watermarking and tree structure based image quality estimation[J]. IEEE Transactions on Multimedia, 2014, 16(2): 311-325.

[11] ZHU X S, DING J, DONG H H, et al. Normalized correlation-based quantization modulation for robust watermarking[J]. IEEE Transactions on Multimedia, 2014, 16(7): 1888-1904.

[12] DONG P, BRANKOV J G, GALATSANOS N P, et al. Digital watermarking robust to geometric distortions[J]. IEEE Transactions on Image Processing, 2005, 14(12): 2140-2150.

[13] SUBRAMANYAM A V, EMMANUEL S, KANKANHALLI M S. Robust watermarking of compressed and encrypted JPEG2000 images[J]. IEEE Transactions on Multimedia, 2012, 14(3): 703-716.

[14] PEREIRA S, PUN T. Robust template matching for affine resistant image watermarks[J]. IEEE Transactions on Image Processing, 2000, 9(6): 1123-1129.

[15] KANG X G, HUANG J W, SHI Y Q, et al. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 776-786.

[16] COLTUC D, CHASSERY J M. Distortion-free robust watermarking: A case study[C]//Security, Steganography, and Watermarking of Multimedia Contents IX. San Jose: SPIE, 2007: 585-592.

[17] WANG X, LI X L, PEI Q Q. Independent embedding domain based two-stage robust reversible watermarking[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2406-2417.

[18] GHOSH B R, BANERJEE S, MANDAL J K. Watermark based image authentication using integer wavelet transform[C]//2022 International Conference on Inventive Computation Technologies (ICICT). Piscataway: IEEE, 2022: 312-319.

[19] LIANG X Y, XIANG S J, YANG L, et al. Robust and reversible image watermarking in homomorphic encrypted domain[J]. Signal Processing: Image Communication, 2021, 99: 116462.

[20] LIU X Y, LOU J T, FANG H, et al. A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images[J]. IEEE Access, 2019, 7: 76580-76598.

[21] TANG Y C, WANG S, WANG C T, et al. A highly robust reversible watermarking scheme using embedding optimization and rounded error compensation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(4): 1593-1609.

[22] HU R W, XIANG S J. Cover-lossless robust image watermarking against geometric deformations[J].IEEE Transactions on Image Processing, 2021, 30: 318-331.

[23] 李赵红, 黄亮, 张文礼. 用于二值图像认证的数字水印技术[J]. 北京邮电大学学报, 2010, 33(5): 66-69, 74.
LI Z H, HUANG L, ZHANG W L. An authentication watermarking technique for binary images[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(5): 66-69, 74. (in Chinese)

[24] 岳桢, 李子臣, 杨义先, 等. 直方图2Bin多进制图像数字水印算法的研究[J]. 电子学报, 2020, 48(3): 531-537.
YUE Z, LI Z C, YANG Y X, et al. A histogram-based 2Bin M-ary image digital watermarking algorithm[J]. Acta Electronica Sinica, 2020, 48(3): 531-537. (in Chinese)

[25] FU D H, ZHOU X Y, XU L R, et al. Robust reversible watermarking by fractional order zernike moments and pseudo-zernike moments[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(12): 7310-7326.

[26] GISHKORI S, MULGREW B. Pseudo-zernike moments based sparse representations for SAR image classification[J]. IEEE Transactions on Aerospace and Electronic Systems, 2019, 55(2): 1037-1044.

[27] 张天骐, 叶绍鹏, 周琳. 一种压缩感知下的NSCT-Zernike的鲁棒数字水印方案[J]. 北京理工大学学报, 2022, 42(2): 208-214.
ZHANG T Q, YE S P, ZHOU L. A robust digital watermarking of NSCT-zernike under compressed sensing[J]. Transactions of Beijing Institute of Technology, 2022, 42(2): 208-214. (in Chinese)

[28] KAMILA N K, MAHAPATRA S, NANDA S. RETRACTED: Invariance image analysis using modified Zernike moments[J]. Pattern Recognition Letters, 2005, 26(6): 747-753.

[29] LIAO S X, PAWLAK M. On the accuracy of Zernike moments for image analysis[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20(12): 1358-1364.

[30] PAWLAK M, LIAO S X. On the recovery of a function on a circular domain[J]. IEEE Transactions on Information Theory, 2002, 48(10): 2736-2753.

[31] XIN Y Q, LIAO S, PAWLAK M. Circularly orthogonal moments for geometrically robust image watermarking[J]. Pattern Recognition, 2007, 40(12): 3740-3752.

[32] SACHNEV V, KIM H J, NAM J, et al. Reversible watermarking algorithm using sorting and prediction[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(7): 989-999.

[33] WANG H D, YAO H, QIN C, et al. When robust reversible watermarking meets cropping attacks[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2024, 34(12): 13282-13296.

[34] SUN Y, YUAN X C, LIU T, et al. FRRW: A feature extraction-based robust and reversible watermarking scheme utilizing zernike moments and histogram shifting[J]. Journal of King Saud University-Computer and Information Sciences, 2023, 35(8): 101698.

作者简介

高光勇　男, 1973年7月出生, 江西九江人. 南京信息工程大学计算机学院教授. 主要研究方向为可逆数据隐藏、计算机网络安全、多媒体信息安全、数字图像处理等.
E-mail: gaoguangyong@163.com

花　锋　男, 1999年9月出生, 江苏盐城人. 南京信息工程大学软件学院硕士研究生. 主要研究方向为信息隐藏、鲁棒可逆水印.
E-mail: 865126814@qq.com

王　敏　女, 1997年11月出生, 安徽滁州人. 南京信息工程大学软件工程硕士. 主要研究方向为鲁棒可逆水印.
E-mail: wangminstu@163.com

赵传信　男, 1977年11月出生, 安徽凤阳人. 安徽师范大学教授, 博士生导师. 主要研究方向为物联网能量优化、智能信息处理、物联网安全等.
E-mail: zhaocx@ahnu.edu.cn

夏志华　男, 1983年9月出生, 湖南常德人. 暨南大学网络安全学院教授. 主要研究方向为数字取证和加密图像处理. 中国电子学会会员编号:E190087278M.
E-mail: xia_zhihua@163.com