数字图像多功能水印综述

赵蕾, 桂小林*, 邵屹杨, 戴慧珺

[1] (西安交通大学电子与信息学部 西安 710049)
[2] (陕西省计算机网络重点实验室 西安 710049)
(xlgui@mail.xjtu.edu.cn)

摘 要: 数字图像多功能水印技术通过将多种类型的水印嵌入到同一图像, 以实现 2 种及以上的图像保护功能(版权保护、内容认证、篡改恢复等). 当前, 数字图像多功能水印算法仍面临着性能和应用场景等方面的挑战. 为促进图像多功能水印的进一步发展, 首先系统地梳理了数字图像水印技术, 包括其系统特性、常见分类、关键技术与成果, 以及其可实现的功能与应用场景; 在此基础上, 对近 10 年来不同类别的多功能水印嵌入模型(融合水印嵌入、零水印嵌入、水印串行嵌入、水印并行嵌入)的相关工作进行归纳与分析; 最后, 总结了当前数字图像多功能水印技术的不足, 展望了后续研究与发展趋势. 综合分析发现, 多水印的嵌入难免对水印综合性能造成损失, 且多功能水印在真实应用场景中的效果仍待改善. 人工智能等新技术在数字图像多功能水印中的应用有望提升算法性能.

关键词: 数字图像水印; 多功能水印; 版权保护; 内容认证; 篡改恢复
中图法分类号: TP391.41 **DOI:** 10.3724/SP.J.1089.2024.20078

Survey on Multipurpose Digital Image Watermarking

Zhao Lei, Gui Xiaolin*, Shao Yiyang, and Dai Huijun

[1] (*Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an* 710049)
[2] (*Shaanxi Province Key Laboratory of Computer Network, Xi'an* 710049)

Abstract: Multipurpose image watermarking aims to provide two or more image protection functionalities by embedding various types of watermarks into the same image, including capabilities of copyright protection, content authentication, and tampered recovery. But it still faces challenges in terms of performance and application scenarios nowadays. To promote the study of multipurpose image watermarking, this paper reviews digital image watermarking first, covering its system characteristics, classifications, key technologies, achievable functions, and application scenarios. Furthermore, multipurpose image watermarking methods developed in the past decade are compared and analyzed in terms of fusion-watermark embedding, zero-watermark embedding, serial-watermark embedding, and parallel-watermark embedding. Finally, the future research prospects and development trends are discussed. It is important to note that embedding multiple watermarks results in performance losses in most cases, and further improvements are needed to enhance its effectiveness in real-world application scenarios. Leveraging artificial intelligence techniques in image multipurpose watermarking holds the promising potential to enhance performance.

收稿日期: 2022-11-21; 修回日期: 2023-06-14. **基金项目**: 国家重点研发计划(2022YFB3305502); 陕西省自然科学基础研究计划(重点计划)(2023-JC-ZD-38). **赵蕾**(1999—), 女, 硕士研究生, 主要研究方向为图像水印、隐私保护、数据挖掘; **桂小林**(1966—), 男, 博士, 教授, 博士生导师, CCF 高级会员, 论文通信作者, 主要研究方向为物联网、云计算、大数据分析与隐私保护、信息安全; **邵屹杨**(1992—), 男, 博士研究生, 主要研究方向为云计算、信息安全、深度学习; **戴慧珺**(1979—), 女, 博士, 讲师, 主要研究方向为物联网隐私保护、城市计算、网络安全.

Key words: digital image watermarking; multipurpose watermark; copyright protection; content authentication; tampered recovery

当前, 社交媒体软件(如微信、微博、抖音等)已成为人们生活中不可或缺的一部分, 人们能够通过上述软件完成多媒体信息的实时共享. 在此过程中, 数字图像作为最广泛使用的多媒体信息之一, 能够通过图像编辑软件、截图软件等被自由地创建、存储、编辑和分发[1]. 这些技术与软件的诞生为人们传递信息、记录日常活动、表达和分享情感提供了便利, 但同时也引发了一系列信息安全问题. 一方面, 攻击者可以对传输中的数字图像实施篡改, 严重威胁图像信息的真实性和完整性. 若被篡改的图像涉及国家安全、法庭证据、医疗诊断等重要领域, 会造成不可预知的严重后果. 另一方面, 原创的数字图像可以被盗版者轻易复制、修改、重新传播, 最终混淆作品的版权所属. 这严重打击了创作者的积极性, 有损数字内容市场健康. 因此, 数字图像的版权保护、真实性和完整性保护是相关领域不容忽视的问题.

水印技术在过去的几十年里得到深入研究与广泛应用, 被证明是解决上述问题的有力机制[2]. 数字图像水印技术作为其重要分支, 通过把具有特定意义的图像、文本等数字信号隐藏在载体图像的方法[3], 在不破坏载体图像使用价值的前提下, 实现载体图像的版权和所有权保护、内容完整性验证、篡改检测与定位或篡改区域恢复功能.

数字图像水印领域包括 3 个分支: 鲁棒水印用于实现图像版权和所有权保护[4-6], 脆弱和半脆弱水印则致力于分析和定位图像篡改区域[7-9]、认证图像内容[10-12]. 部分水印算法将自恢复技术与脆弱或半脆弱水印结合, 可以在检测、定位篡改的基础上实现篡改区域恢复, 以获得更高级别的安全保护[13-14]. 目前, 研究人员已针对不同功能设计出性能优异的图像水印算法.

近年来, 随着远程医疗、电子政务与商务的发展, 越来越多的应用需要同时实现图像的版权保护、内容完整性和真实性验证等多种功能. 因此, 传统的单功能水印算法已无法满足业务需求, 研究者相继提出了同时实现鲁棒水印与(半)脆弱水印相关功能的多功能图像水印算法[15-17]. 然而, 现有算法通常以增加水印嵌入量为代价实现多功能, 当水印嵌入量增加时, 会影响水印的性能[18]. 目前, 设计高效的数字图像多功能水印算法是研究人员面临的新挑战.

当前, 国内外研究人员对数字图像鲁棒水印、脆弱水印、半脆弱水印算法进行了各种角度的分类与梳理[1,19-21], 但仍缺乏对数字图像多功能水印的综述报道, 本文对这些工作进行总结. 首先, 对数字图像水印技术的基本原理与经典成果进行概述, 特别是对水印实现功能与应用场景进行总结; 其次, 以多功能图像水印算法采用的嵌入模型为分类标准, 归纳、梳理与分析近 10 年的数字图像多功能水印算法, 并以表格形式对各算法的优缺点、采用的嵌入、优化和加密方法、实现的多功能等进行总结; 然后, 对当前数字图像多功能水印算法的整体趋势进行归纳; 最后, 根据多功能图像水印算法面临的挑战给出可能的解决方案, 探究未来发展趋势.

1 数字图像水印技术概述

1.1 数字图像水印系统特性及评价指标

数字图像水印算法在设计时必须结合应用需求, 满足水印系统的基本要求和特性. 图 1 所示为数字图像水印算法设计时遵循的特性, 分别是不可见性、安全性、容量、鲁棒性、定位和可恢复性、可逆性、计算复杂性. 其中, 不可见性是绝大多数算法在设计时需考虑的因素[20], 而其他则在不同类别水印算法和应用场景中有不同侧重.

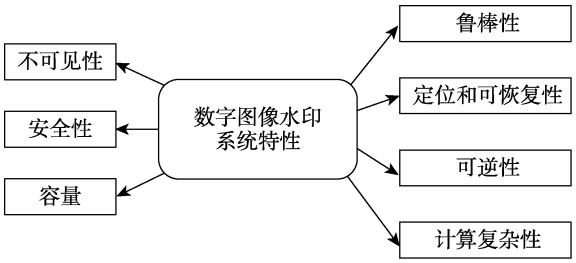


图 1 数字图像水印系统特性

1.1.1 不可见性

不可见性又称为透明性, 指嵌入的水印在人类视觉系统(human visual system, HVS)下无法被察觉, 嵌入后载体图像不发生明显变化.

1.1.2 安全性

安全性一方面指攻击者难以探测载体中包含水印信息, 另一方面指攻击者在没有密钥的情况下即使知道公开的水印算法, 也无法获取水印真

实内容. 多数算法通过在嵌入前加密水印来提高安全性, 混沌映射[22-23], Arnold 变换[24-25]是图像水印常用的加密方法.

1.1.3　容　量

容量指载体中嵌入的水印信息量, 是评价水印系统不可忽视的特性. 容量越大意味着传递的信息越多, 能够实现更复杂的功能. 但容量受限于载体图像的尺寸、水印的嵌入方法和不可见性要求.

1.1.4　鲁棒性

鲁棒性指嵌入水印的载体图像在传播过程中遭受常见信号处理攻击(噪声、滤波、JPEG 压缩、剪切等)或恶意篡改后, 仍能提取出清晰、准确水印信息的能力. 当前, 鲁棒水印算法仍以提高鲁棒性为首要目标, 特别是提高抗几何攻击(旋转、缩放、剪切等)的能力[19].

1.1.5　定位和可恢复性

定位和可恢复性指载体图像遭受修改后, 算法能够准确判断载体是否篡改、定位篡改区域与恢复篡改区域的能力. 脆弱、半脆弱水印大多具备此特性.

1.1.6　可逆性

可逆性指提取水印后能无损恢复原载体图像的能力. 对于医学、军事、司法图像而言, 即便嵌入少量水印信息也可能影响图像的后续使用. 因此, 为保证载体内容精确性, 水印实现相关功能后需将载体图像恢复原状. 具备此特性的水印称作可逆水印, 其亦为水印领域重要分支之一.

可逆性的实现基于图像像素之间的高度相关性和大量冗余, 该特性使图像可以被高度压缩, 以更小的空间表示. 可逆算法“压缩”图像并将水印信息填补在压缩后的空余空间, 提取水印后将图像进行“复原”. 无损数据压缩、差值扩展算法、整数变换、预测残差扩展、直方图移位等[26]是实现可逆水印的代表性方法. 可逆信息隐藏技术详见文献[26].

1.1.7　计算复杂性

计算复杂性反映水印嵌入和提取过程的计算复杂度. 水印算法应用在实时性要求高的工业物联网场景时需要格外关注此特性.

1.1.8　数字图像水印系统特性总结

上述水印系统特性难以被某个算法同时满足, 多数情况下研究者只能根据使用场景和实现功能侧重于提高某些特性的性能, 设计出最符合相关应用场景的水印算法.

另外, 在数字图像水印领域, 部分重要特性存在公认的客观评价指标. 水印嵌入后的不可见性通常由峰值信噪比(peak signal to noise ratio, PSNR)、结构相似度(structural similarity index metric, SSIM)指标衡量, PSNR 和 SSIM 的值越大表示含水印载体图像质量越高. 水印的鲁棒性通过归一化互相关系数(normalization cross correlation, NCC)、误码率(bit error rate, BER)计算, 当原水印与提取水印之间的 NCC 越接近于 1 或 BER 越接近 0 时, 水印具有强鲁棒性. 每像素位数通过计算载体图像每像素蕴含的水印信息位数反映水印嵌入量. 漏警率、虚警率、正确率评价水印篡改检测与定位的精度[1].

1.2　数字图像水印常见分类

图 2 所示为数字图像水印常见分类方式, 根据水印的鲁棒性、提取方式、嵌入域、载体图像类型进行划分.

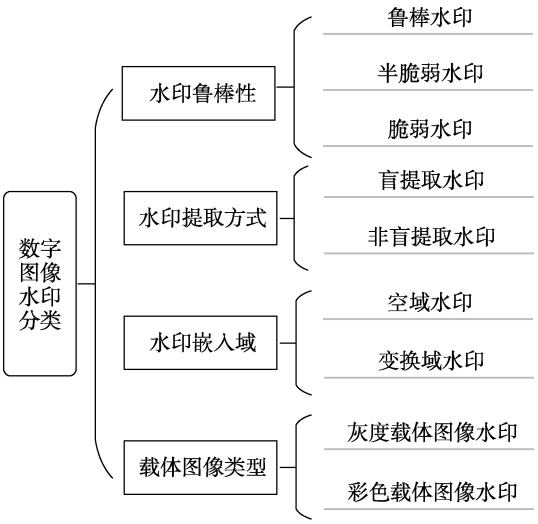


图 2　数字图像水印分类

根据水印的鲁棒性可将水印分为鲁棒水印、脆弱水印、半脆弱水印. 鲁棒水印具有强鲁棒性, 攻击者无论如何修改、压缩、转换载体图像, 水印信息都尽可能地保留. 脆弱水印缺乏鲁棒性, 当载体图像发生像素级细微修改时, 水印就会被破坏. 半脆弱水印的鲁棒性介于二者之间, 能够抵抗 JPEG 压缩、基础图像处理等内容保留修改, 对恶意篡改图像内容操作敏感.

根据提取水印时是否需要原载体图像、水印信息, 可将水印分为盲提取水印和非盲提取水印. 盲提取水印也称作公有水印, 指水印提取时不需要原载体图像和水印信息参与, 只需密钥就能够完整提取并恢复水印信息[27]. 非盲提取水印亦称私有水印, 指提取时除了密钥, 还需原载体图像或水

印信息才能恢复嵌入信息的水印, 其实施时需要额外在可信第三方机构存储载体图像或水印信息. 从经济性和实用性角度讲, 盲提取水印相比非盲提取水印的应用范围更广、适应能力更强.

根据水印嵌入区域的不同, 可将水印分为空域水印与变换域水印. 直接嵌入到载体图像原始像素中的水印称为空域水印, 嵌入到载体图像经信号变换后系数中的水印为变换域水印. 由于空域嵌入的水印鲁棒性欠佳, 常用于实现脆弱水印算法. 变换域水印具有更强的鲁棒性, 常用于实现鲁棒水印算法.

根据载体图像类型可将水印算法分为灰度图像水印与彩色图像水印算法. 灰度图像水印算法较为成熟, 将该类水印算法应用于彩色图像不同的颜色通道, 可以实现灰度图像水印算法到彩色图像水印算法的推广, 但这种简单的推广难以发挥彩色图像的特点与优势. 彩色图像可用不同的颜色模型进行表示, 如 RGB, HSV, HSL, CMYK, CIE Lab, YUV, YCbCr 等, 选取合适的模型进行水印嵌入在一定程度上能够提升算法性能. 目前, 在彩色图像水印算法, RGB 与 YCbCr 颜色模型的应用最为广泛[19,28-29]. 数字图像水印详细分类见文献[30].

1.3 数字图像水印关键技术

表 1 对数字图像水印算法的关键技术进行了全面总结, 涵盖水印嵌入域、水印嵌入与提取方法、水印优化方法 3 个方面, 并对各方面进行详细分类与优缺点归纳; 同时, 将所述文献分类, 以便于读者快速定位相关信息. 为了更好地理解水印算法的实现细节, 还对表 1 所列技术与相关成果进行概述.

1.3.1 水印嵌入域

水印可以嵌入在载体图像的空域或变换域. 空域指载体图像的原始像素矩阵, 变换域指图像通过某种频域变换、矩阵分解方法得到的频谱、分解矩阵. 嵌入域的选择初步决定了水印的基本性能, 是算法至关重要的一环.

(1) 基于空域的水印算法

空域水印算法根据水印信息直接修改载体图像像素完成水印嵌入. 最初的水印算法基于空域提出, 最低有效位(least significant bit, LSB)和 Patchwork 是其中 2 类经典的算法.

LSB 类算法的核心是将水印信息替换至载体图像最低位组成的位平面. 由于最低位数据权重较低, 发生变动后对载体图像质量的影响微乎其微, 因此, 水印具有较高的不可见性. van Schyndel 等[31]最早提出将 LSB 应用于数字图像水印. 此类算法易于实现, 嵌入水印容量大且计算复杂度低, 但往往滤波、噪声、压缩等普通攻击就可破坏嵌入的信息. 为了提高水印鲁棒性, Zhang 等[32]和 Badran 等[33]将小水印重复多次嵌入在载体的不同区域, 保证图像遭受攻击后至少可恢复出 1 个完整的水印; Zeki 等[34]和 Mohammed 等[35]将水印嵌入在能量较大的中间有效位平面来提高鲁棒性, 但对载体的质量有较大影响. 尽管还有方法可以提高 LSB 类算法的鲁棒性[36-37], 但在此类方法中, 任何干扰与攻击都会轻易使图像像素发生改变, 嵌入水印的脆弱性是不可忽略的事实, 因此, 目前鲁棒水印算法大多放弃此方法, 脆弱、半脆弱水印算法则充分利用该特点, 在 LSB 类算法的基础上扩展出一系列能够实现载体图像篡改检测与定位的水印算法[13,38], 使 LSB 类算法在诞生的 30 年后仍旧焕发着生机.

与 LSB 类算法不同, Patchwork 类算法基于载体图像统计特性. Bender 等[39]将水印信息融合在载体图像的亮度统计特性中. 该算法随机从载体图像中选取 2 个像素集合 A 和 B, 并根据水印嵌入值提高(降低)集合 A 中所有像素的亮度, 同时降低(提高)集合 B 中所有像素的亮度, 从而实现 1 bit 水印信息的嵌入. 相比于 LSB 类算法, Patchwork 类算法提高了嵌入水印的鲁棒性, 在一定程度上能够抵抗非几何攻击. 但由于水印嵌入容量较小, 该算法逐渐被放弃.

(2) 基于变换域的水印算法

为了弥补空域水印算法的缺陷, 基于变换域的算法应运而生. 该类算法将载体图像转化到变换域后, 根据水印值修改变换域系数嵌入水印. 变换域系数的变化会均匀扩散到载体图像的所有像素, 因此, 水印嵌入后不可见性较高. 同时, 大量像素改变才会导致变换域系数发生较大变化, 因此, 水印的鲁棒性也能得到大幅提升. 图像水印算法最常用的变换有离散傅里叶变换(discrete fourier transform, DFT)、离散余弦变换(discrete cosine transform, DCT)、离散小波变换(discrete wavelet transform, DWT)、奇异值分解(singular value decomposition, SVD)等.

DFT 在数字信号处理领域占据重要地位. 图像经过 DFT 可分解为幅频分量与相频分量, 幅频分量具有平移不变性[19], 水印信息嵌入此区域可获得较强抵抗几何攻击的能力[40]. 在幅频分量中,

中低频系数的较大值处集中了较多能量, 将水印信息嵌在这些系数中可获得更高的鲁棒性, 同时保证了水印嵌入的不可见性[41]. 但 DFT 是一种全局变换, 不能刻画信号的局部特性, 在处理图像之类的非平稳信号和突变信号时效果不佳且与国际图像压缩标准不兼容. 因此, 当前 DFT 类水印算法应用较少.

DCT 的能量压缩特性使其成为图像和视频处理领域的常用技术. 图像进行 DCT 后, 可以得到直流、低频、中频、高频成分[42]. 直流成分代表图像平均亮度信息, 集中绝大多数能量. 在高能量区域嵌入水印的鲁棒性强, 但严重影响载体图像的视觉质量. 因此, 多数算法选择在中低频嵌入水印, 实现鲁棒性和不可见性之间的平衡. Cox 等[43]首次提出了基于 DCT 的数字图像水印算法, 将水印信息扩频后嵌入载体图像 DCT 后的 1 000 个低频系数上. 实验证明, 水印可以抵抗一定程度的 JPEG 压缩, 但全局 DCT 对于大尺寸图像而言运算复杂度高. 针对上述问题, 同时考虑到 JPEG 压缩中使用的区块尺寸, 多数算法选择将图像分为互不重叠的 8×8 区块后再进行 DCT 与水印嵌入, 以得到更好的效果[44-46]. 基于 DCT 的水印能够抵抗大部分常见攻击, 尤其是与图像压缩技术结合后抵抗 JPEG 压缩攻击效果好, 然而, 它容易受到剪切、缩放等几何攻击的破坏[47]. 而且与 DFT 相同, DCT 也是一种全局变换, 不能妥善刻画信号的局部特性.

DWT 是一种时域频域多分辨率分析方法, 在信号频域变换的同时保留了时域的特点, 能够妥善对非平稳信号和突变信号进行局部化分析[48]. 数字图像经过 DWT 能够实现多方向、多分辨率分解, 即图像可以分解成不同空间、不同频率、不同方向的 4 个频带: 低频子带(low-low, LL)、水平子带(high-low, HL)、垂直子带(low-high, LH)和对角子带(high-high, HH)[49]. 低频部分保留原图绝大部分信息, 集中了极高能量. 高频部分 HL, LH, HH 为图像的细节与边缘信息, 能量较少. LL 可以继续执行 DWT, 实现多级分解. 在基于 DWT 的图像水印算法中, 选择不同的分解级数、嵌入位置和嵌入强度能够灵活调整水印的鲁棒性与不可见性. 将水印信息嵌入 LL 区域, 可以确保水印的鲁棒性, 但容易引起图像降质; 将水印信息嵌入 HL, LH, HH 区域, 水印的鲁棒性不佳, 但可维持原载体图像的质量[50-51]. 多年来, 对 DWT 的应用一直是数字水印领域的重点. 随着对第一代传统小波变换的修改与完善, 具备新特性的提升小波变换(lifting wavelet transform, LWT)[52]、整数小波变换(integer wavelet transform, IWT)[53]、稳定小波变换(stationary wavelet transform, SWT)[54]、冗余小波变换(redundant wavelet transform, RDWT)[55]、双数复小波变换[56]等也被应用在数字图像鲁棒水印算法.

基于 DFT, DCT, DWT 的水印大多能抵抗常见信号处理攻击、JPEG 压缩攻击, 但对旋转、缩放、剪切等几何攻击效果不佳, 因此, 具有几何不变性的矩阵变换被应用在水印算法. SVD 是当前数字图像水印领域应用最为广泛的矩阵分解技术. 图像经过 SVD 可分解为 3 个矩阵的乘积, 公式为

$$\boldsymbol{A}=\boldsymbol{U}\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}}=[\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_N]\times\begin{bmatrix}s_1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & s_N\end{bmatrix}\times[\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_N] \tag{1}$$

其中, $\boldsymbol{A}$ 为待分解图像; $\boldsymbol{S}$ 为图像奇异值组成的对角矩阵, 表示图像亮度信息; $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 矩阵是 $\boldsymbol{S}$ 的左右特征向量, 表示图像几何信息.

$\boldsymbol{S}$ 的对角线值轻微改变后, 重构载体图像的变化微乎其微, 因此, 在此区域嵌入水印不会破坏载体图像视觉质量. 同时, SVD 的特征向量具有转置、旋转、位移不变性, 具有良好的稳定性和抗噪性. 将水印信息嵌入在奇异值矩阵中, 水印抗几何攻击能力强[30]. Liu 等[57]对载体图像实施 SVD, 根据水印信息修改奇异值矩阵完成水印嵌入. 实验结果证明水印抵抗几何攻击的能力比同期鲁棒水印算法强. 蔡宜嘉等[58]对载体图像进行分块 SVD, 在每一块 $\boldsymbol{S}$ 矩阵上选择系数进行嵌入, 同样实现了较好的效果. 但 SVD 的计算复杂度较高, 随后, 基于矩阵三角(lower-upper, LU)分解[59], Schur 分解[60], QR 分解[61]和 Hessenberg 分解[62]的水印算法被提出. Schur 分解是 SVD 的中间步骤, 计算量是 SVD 的三分之一. QR 分解从理论上讲时间复杂度更小, 而 Hessenberg 分解是 QR 分解的中间步骤[63]. 采用这些分解方法一定程度上能够提高水印算法的执行效率, 更适合应用在实时性要求高的场景中.

随着多尺度几何分析理论的出现, 数字图像水印算法被注入了新的活力. Do 等[64]提出了一种多分辨率变换, 轮廓波变换(contourlet transform, CT). 该变换可以将图像分解为 3 个方向以上的子带, 较传统小波变换能够更好地表示图像几何结构, 被应用于部分图像水印算法[65-66]. 剪切波变换(shearlet transform, ST)较 CT 具有更简单的数学结构, 为图像的几何表示提供了更加灵活的选择, 再

加上其多分辨率特性和近最优非线性逼近性能, 最近几年也被多数算法选择[67].

传统的小波变换仅递归分解低频成分, 未对纹理细节较为丰富的高频子带继续进行处理, 添加水印时没有充分利用纹理复杂性去提高水印不可见性. 小波包变换则实现了高频部分的无冗余、无疏漏分解, 对中、高频成分更好地进行时频局部化分析, 应用在图像水印算法可提高水印不可见性[29]. 斜波变换(slantlet transform, SLT)相对于传统小波变换, 在设计上具备更大的灵活度, 可以更好地改善信号时域局部性, 逐渐被使用在图像水印算法[68-69].

为了充分利用频域变换和矩阵分解的优势, 更好地提升水印鲁棒性与不可见性, 将水印嵌入在常用变换相结合的混合变换域是目前图像水印方案的首选. 基于 DWT-DCT[70-71], DWT-SVD[72-73], DWT-DCT-SVD[74-75]嵌入水印是图像水印算法中常见方案, 能够显著地提高水印鲁棒性.

1.3.2 水印嵌入与提取方法

(1) 简单融合与提取

选择合适的嵌入域后, 如何将水印信息与载体图像融合也是算法关键. 简单融合是早期图像水印常用方法, 也称为扩频嵌入方法, 由 Cox 等[76]提出的 3 个公式发展而来, 公式为

$$I' = I + \alpha \times W \tag{2}$$

$$I' = I \times (1 + \alpha \times W) \tag{3}$$

$$I' = I \times \mathrm{e}^{\alpha W} \tag{4}$$

对应提取公式为

$$W' = (I' - I)/\alpha \tag{5}$$

$$W' = (I' - I)/\alpha I \tag{6}$$

$$W' = (\ln I' - \ln I)/\alpha \tag{7}$$

其中, I 指原载体图像频域或空域的系数; I' 指嵌入水印后的系数; W 指待嵌入的水印信息; W' 指提取的水印信息; α 指水印嵌入强度.

式(2)与式(5)、式(3)与式(6)、式(4)与式(7)的简单融合方式分别称作加性融合、乘性融合与指数融合. 此类嵌入与提取方法十分简单, 将水印信息按比例缩放后与载体系数结合即可, 而且适用性强, 能够将十进制像素值不做任何转变直接嵌入载体图像. 但提取水印时, 需要原载体图像作为参考, 无法实现盲提取. 因此, 在要求实现盲提取的场景中并不适用. 此外, 嵌入强度影响着水印最终的鲁棒性和不可见性, 如何设置强度值是该方法的关注点.

(2) 量化嵌入与提取

Chen 等[77]最早提出使用量化索引调制方法嵌入水印信息. 此类方法根据水印信息使用不同的量化器将载体图像像素值量化到不同的量化区间完成嵌入. 提取时根据像素值所在的量化区间确定隐藏的水印信息. 与简单融合方法相比, 它最大的优点是实现了水印的盲提取. 方法中量化步长与相关阈值值得关注, 它们同样影响了水印的鲁棒性和不可见性.

抖动调制(dither modulation, DM)[78]是实现量化嵌入的典型方法, 被广泛应用在图像水印算法. 采取此方法嵌入的水印鲁棒性较强, 但抵抗噪声攻击能力弱, 随后, 扩展变换抖动调制(spread transform dither modulation, STDM)被应用于水印算法. STDM 不直接修改载体图像, 而是对载体图像在随机信号方向的投影所得数据进行抖动调制, 一定程度上提高了嵌入水印的鲁棒性和不可见性[79]. Hatoum 等[80]采取修正的 STDM 方法嵌入水印, 提高了水印抵抗固定增益攻击的能力. Pérez-González 等[81]提出比率抖动调制嵌入方法, 将载体与关于水印某个函数值的比值作为新信号进行量化, 在改善水印性能的同时保证了计算性能接近原始 DM. 除此之外, 对数量化索引调制被设计用于提高水印不可见性[82]. 部分算法则将量化与视觉模型相结合, 改善水印嵌入后的视觉效果[83-85].

(3) 基于元素关系嵌入与提取

基于元素关系的嵌入方法根据水印调整嵌入域一对系数或一些系数的值, 使这些系数值维持一定的关系, 提取时根据值的关系确定隐藏的水印信息. 此方法同样实现了盲提取, 最近几年被广泛应用在图像水印算法. 选择载体图像上 2 个特定值的相对大小关系代表隐藏的水印信息是此类嵌入方法常用的规则. 文献[86-87]通过

$$p_{\mathrm{mean}} = (p_{a,b} + p_{c,d})/2 \tag{8}$$

$$\begin{cases} \begin{cases} p'_{a,b} = p_{\mathrm{mean}} + T/2 \\ p'_{c,d} = p_{\mathrm{mean}} - T/2 \end{cases}, & \text{if } W=1 \\ \begin{cases} p'_{a,b} = p_{\mathrm{mean}} - T/2 \\ p'_{c,d} = p_{\mathrm{mean}} + T/2 \end{cases}, & \text{otherwise} \end{cases} \tag{9}$$

调整系数大小完成水印嵌入. 其中, p_{mean} 是随机选取 2 个像素 $p_{a,b}$ 与 $p_{c,d}$ 的均值; W 是待嵌入的水印位, 取值为 0 或 1; 参数 T 能够调节水印鲁棒性和不可见性; $p'_{a,b}$ 与 $p'_{c,d}$ 为修改后的像素值. 对应水印提取公式为

$$W' = \begin{cases} 1, & \text{if } p'_{a,b} > p'_{c,d} \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

其中, W' 是根据 2 个像素大小关系提取的水印位.

这种调整方式是很多基于元素关系嵌入与提取方法的基础. 此类方法需要注意选定系数的原始值, 若值相差过大, 嵌入时对载体图像的改动就大, 易降低载体图像质量. 在苏庆堂[63]提出的算法中, 选择数值相近的系数嵌入水印可获得更好的性能. 部分算法通过调整 2 个区域均值大小完成水印嵌入, 水印具有更强的鲁棒性[88].

(4) 零水印

零水印与上述方法相比, 是一种不对载体图像做任何修改的"嵌入"方法[89]. 根据载体图像的特征构造水印信息, 并将加密后的水印存储在可信第 3 方机构. 验证时, 采用相同方式构造水印信息, 与第 3 方存储的信息比对后就能够实现版权/所有权的认证或篡改检测. 零水印的鲁棒性取决于构造水印时依赖的载体特征. 当特征足够鲁棒时, 水印能够实现鲁棒水印的相关功能; 比较脆弱时, 能够实现脆弱水印的相关功能. 零水印嵌入的最大特点是不改变原载体图像, 充分保证了载体图像质量, 适合应用在对图像质量有严格要求的医学、军事领域[90].

(5) 基于深度学习嵌入与提取

随着深度学习尤其是计算机视觉的迅速发展, 数字图像水印技术也在不断创新. 传统水印的嵌入与提取方法依赖具体的数学函数实现, 需要研究者具备数学与信号处理知识才能将水印信息与载体图像较好地融合. 基于深度学习的嵌入与提取方法不再需要手动设计复杂的数学函数, 而是通过大量数据训练神经网络去融合和分离水印与载体图像[91], 嵌入与提取过程接近黑盒.

2017 年, Kandi 等[92]提出一种基于卷积神经网络(convolutional neural network, CNN)自编码器的深度学习鲁棒水印算法. 将神经网络作为水印嵌入编码模块的一部分, 自动寻求合适的水印嵌入区域. 但该方法属于非盲水印算法, 且训练过程中未考虑攻击情况, 鲁棒性较差. 同年, Mun 等[93]利用神经网络的自适应能力, 将其应用在水印提取端以提高解码性能.

不久后, 受 AlexNet[94]的影响, 基于端到端的水印嵌入与提取算法被提出. Hayes 等[95]基于生成式对抗网络(generative adversarial network, GAN)设计出一种端到端的水印模型, 该模型由生成器、提取器和隐写分析器组成. 其中, 生成器将 n 位二进制信息隐藏至载体图像; 提取器从嵌入水印的图像中提取隐藏信息; 隐写分析器判别载体是否为生成图像. 通过对抗学习, 水印获得较强的隐藏能力. Zhang 等[96]于 2019 年提出 SteganoGAN, 设计了与上述框架相似的水印算法, 仅在网络结构上略有差别. 但上述算法在设计时未考虑攻击因素, 因此, 水印鲁棒性不佳.

2018 年, Zhu 等[97]提出一种端到端的可训练盲水印模型 HiDDeN, 创造性地在网络训练过程中加入可微噪声层模拟各类攻击以提升水印鲁棒性. 图 3 所示为该模型结构简化图, 包括基于卷积-批量归一化-ReLU 结构的编、解码器和对抗性鉴别器以及 1 个噪声层. 编码器负责将二进制水印信息与载体图像通过拼接与多层卷积进行融合, 输出含水印载体图像; 噪声层对其进行 Dropout, Cropout 等攻击后送入解码器提取水印信息; 鉴别器负责评判图像含水印的概率. 各模块联合训练, 以最小化图像重建损失、水印重建损失与图像鉴别损失为目标. 该算法在保证信息嵌入容量的情况下实现了较好的不可见性与鲁棒性, 同时, 改变了以往信息隐藏的思路, 将基于深度学习模型的水印算法推进了新阶段.

随后, 不少工作基于 HiDDeN 框架进行改进, 集中在修改噪声层、网络结构和对抗训练策略 3 个方面. Ahmadi 等[98]在 HiDDeN 框架下提出一种基于残差结构和 CNN 实现的水印框架 ReDMark, 对噪声模拟层的 JPEG 有损压缩进行了改进, 最终提高了水印嵌入的不可见性和鲁棒性. Jia 等[99]在 Zhu 等[97]和 Liu 等[100]的 JPEG 压缩模拟攻击基础上结合真实 JPEG 压缩攻击, 提出在训练时对不同批次数据采用不同类型的 JPEG 压缩模拟攻击方式, 有效提高了水印抵抗 JPEG 压缩能力. Hamamoto 等[101]设计出一种模拟旋转攻击方案, 提升了水印抵抗旋转攻击的能力. Luo 等[102]则利用 CNN 模拟不同的几何与噪声攻击, 同时, 使用对抗训练的方式代替指定攻击训练, 从而实现抵抗未知攻击的能力. Tancik 等[103]提出 StegaStamp 网络结构, 模拟了如颜色变化、模糊等更真实的图像攻击手段. 最终, 即便图像打印或手机重摄后也能检测出水印信息, 水印鲁棒性得到增强. Ge 等[104]基于端到端的模型针对文本图像提出一种抗屏幕拍摄攻击的水印嵌入与提取方案. 其中, 失真层模拟了拍摄照片时易产生的相机失真、拍摄失真及光源失真. 使用该方法后, 即便文本图像被盗摄, 也依旧能够从盗摄图像中提取水印信息. 此外, 模型训练过程中加入了背景敏感损失、Lpips 损失[105]与嵌入强度调整策略, 共同提高了水印嵌入后的不可见性.

Liu 等[106]对 HiDDeN 结构进行改进, 无需考

虑噪声层, 提出了两阶段分离的盲水印实现框架. 该模型在不考虑噪声的情况下训练编码器, 在考虑噪声的情况下调整解码器参数, 最终有效提高水印抵抗未知噪声攻击的能力.

Zhang 等[107]对通用深度学习水印框架中的攻击网络进行探究, 提出一种前向传播的攻击网络层, 提高水印嵌入后的鲁棒性. 最终, 提高了水印抵抗不可微或黑盒失真的能力.

此外, 为了提高水印嵌入后的不可见性, Yu[108]通过 ResNet50 学习输入载体图像的注意力掩膜, 将载体图像、水印图像与注意力掩膜融合生成视觉质量更好的含水印图像, 本质上将水印嵌入了人类视觉不敏感位置. Hao 等[109]在鉴别器前增加高通滤波器结构, 最终使水印倾向于嵌入图像的中频区域, 避免嵌入低频区域影响载体质量.

使用深度学习模型实现的水印嵌入与提取方

表 1 数字图像水印关键技术总结

数字图像水印关键技术	分类	细化分类	文献	优点	缺点
水印嵌入域	空域	LSB 类	[31-38]	水印嵌入容量大且计算复杂度低; 嵌入后不可见性较高	水印极易被破坏
		Patchwork 类	[39]	水印鲁棒性较 LSB 类略有提升	水印嵌入容量有限
	变换域	DFT 类	[40-41]	能够抵抗几何攻击	抵抗非几何攻击能力相对较弱
		DCT 类	[42-47]	DCT 的能量聚集特性使得嵌入水印抵抗普通攻击能力强	抵抗几何攻击能力相对较弱
		DWT 类	[48-56]	DWT 的时域频域多分析能力使得嵌入水印在鲁棒性与不可见性之间得到较好权衡	抵抗几何攻击能力相对较弱
		矩阵变换类	[57-63]	能够抵抗几何攻击	通常与 DCT, DWT 结合, 否则抵抗非几何攻击能力较差
		多尺度几何变换类	[65-67]	较 DWT 具有多方向分解特性, 能够提供更多水印嵌入区域	鲁棒性通常较 DWT 类差
水印嵌入与提取方法	简单融合与提取		[76]	方法简单; 可嵌入大容量水印	非盲提取
	量化嵌入与提取		[77-85]	能够实现盲提取	方法设计较为复杂; 水印嵌入容量有限
	基于元素关系嵌入与提取		[26,86-88]	方法简单; 能够实现盲提取	水印嵌入容量有限
	零水印		[89-90]	未真正嵌入水印, 不可见性极高	相关功能的实现需要可信第 3 方机构协助
	基于深度学习嵌入与提取		[92-93,95-109]	能够保证水印的不可见性与鲁棒性; 能够针对不同攻击设计特有的水印嵌入模型	对计算资源要求较高
水印优化方法	提高水印抗几何攻击能力	几何不变量的几何不变性	[110-111]	具备一定的抗几何攻击能力	水印抗几何攻击能力依赖于所选几何不变量对图像失真的稳健性
		特征点的几何不变性	[112-114]	水印嵌入不可见性较高; 抗几何攻击能力较优	特征点数量有限, 限制了水印嵌入容量
		几何(同步)校正	[115-116]	抗几何攻击能力较优	校正时须使用原载体基准信息进行比对
	灵活选取水印嵌入强度		[72,117-122]	使用启发式算法平衡水印的不可见性与鲁棒性	方法设计较为复杂; 计算复杂度通常较高

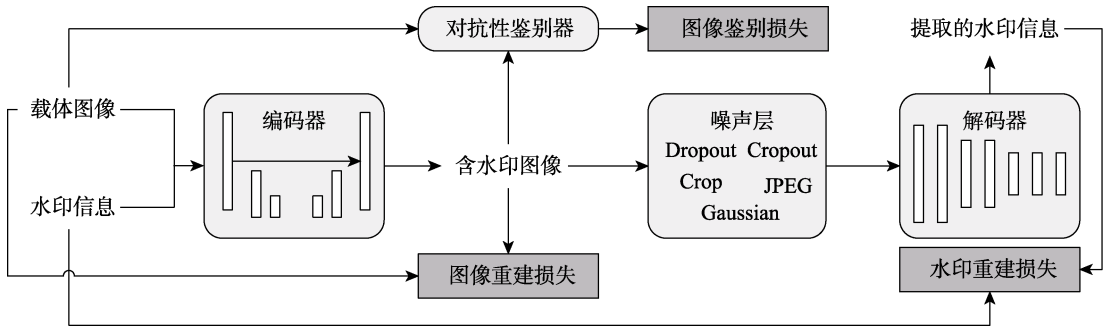


图 3　HiDDeN 模型简化结构

法带来了更强的鲁棒性、更优秀的不可见性与更大嵌入容量, 因此, 是当前单功能水印领域探究热点之一.

1.3.3　水印优化方法

尽管目前多数图像水印算法都具有较好的性能, 但研究人员认为鲁棒水印抵抗几何攻击的能力普遍较差、水印的鲁棒性与不可见性不能得到较好的折中. 因此, 为提升算法的性能, 除了使用第 1.3.2 节基于深度学习嵌入与提取部分提到的相关算法外, 许多研究人员选择从以下角度优化传统水印方案.

(1) 提高水印抗几何攻击能力

多数算法能够较好地抵抗噪声、滤波、压缩等非几何攻击, 但面对旋转、缩放、剪切等几何攻击时效果不佳. 部分学者通过利用图像中几何不变量的几何不变性来保证嵌入水印的鲁棒性. 除了提到的 SVD, Schur 分解外, Zernike 矩、伪 Zernike 矩、复矩、极谐变换(polar harmonic transforms, PHTs)等被证明具有几何不变性的变换也常被应用在图像水印算法, 其中, 对 PHTs 的使用最为常见. Li 等[110]提出了一种基于 PHTs 的算法, 其讨论了 PHTs 的几何不变性, 选择将二值水印嵌入在部分计算精度高的 PHTs 系数. 实验结果表明, 较 Zernike 矩、伪 Zernike 矩类方法, 该水印算法抵抗旋转、缩放攻击效果好且嵌入容量大. Hu 等[111]提出了一种基于 PHTs 和两阶段水印框架的抗几何攻击无损鲁棒水印方法, 配合设计的新量化操作, 水印具有强鲁棒性.

部分学者利用图像特征点的几何不变性, 选择在特征点上嵌入水印. Zhu 等[112]提出了一种基于特征点、多尺度理论和非下采样轮廓波变换(non-subsampled contourlet transform, NSCT)的算法. 使用多尺度 Harris 检测器提取载体鲁棒特征点构造特征区域并将水印嵌入在特征区域 NSCT 后低频系数的伪 Zernike 矩幅值, 使水印具有较高的不可见性和抵抗攻击的能力. 除了 Harris 特征点检测, 尺度不变特征转换(scale-invariant feature transform, SIFT)、加速鲁棒特征(speed-up robust features, SURF)[113-114]等特征检测方法也常用于提高抗几何攻击能力. 特征点的健壮保证了嵌入其上水印的鲁棒性. 但一幅图像中提取的特征点数量有限, 这导致此类方法对嵌入容量有较大限制.

还有部分学者从几何(同步)校正的角度提高水印抗几何攻击能力. 此类方法的核心是通过检测发送与接收端 2 幅图像同一特征的改变, 计算图像几何变换的参数, 从而根据预测参数还原图像, 进行水印提取. Pourhadi 等[115]和李莹莹等[116]分别通过 SIFT 特征匹配点、SURF 特征匹配点的坐标变化推测图像旋转、缩放系数并进行校正. 实验证明水印的抗几何攻击能力得到提升. 但此类算法在校正时必须使用原载体图像或特征信息进行比对, 否则无法恢复图像, 因此, 成为实际应用中的一大限制.

(2) 灵活选取水印嵌入强度

图像水印算法中, 水印鲁棒性和不可见性可通过调整嵌入强度和相关阈值进行控制. 嵌入强度越大, 水印的鲁棒性就越强, 不可见性则越差, 反之亦然. 因此, 为了实现鲁棒性和不可见性之间的平衡, 确定合适的强度值至关重要.

近年来, 学者大多将此视为优化问题, 用启发式优化算法计算水印嵌入的较优强度值. 此类算法的核心是根据水印嵌入后载体的 PSNR 值和模拟多种攻击后水印的 NCC 值构造适应度函数, 在给定约束条件下(通常是 PSNR 的下限, 保证图像的视觉质量), 求出最佳函数值后, 取对应的最优参数作为最终嵌入强度值. 经典的遗传算法(genetic algorithm, GA)[117]、人工蜂群算法(artificial bee colony, ABC)[118]、粒子群算法[119]、蚁群优化算法[115]、萤火虫算法[72]、差分进化[120]、细菌迷失优化算法(bacterial foraging optimization, BFO)[121]等均已被

应用于图像水印. Haghighi 等[122]将一种多目标优化算法, 非支配排序遗传算法(non-dominated sorting genetic algorithm-II, NSGA-II)应用在图像水印: 根据模拟水印嵌入后得到的均方误差(mean square error, MSE)和多种攻击后水印的 NCC 值构造多个目标函数, 得到关于水印嵌入强度的一个权衡解, 达到帕累托最优. 实验结果表明, 水印在保证不可见性的同时具有较高的鲁棒性.

2 数字图像水印实现功能与应用场景

在正式介绍数字图像多功能水印算法前, 有必要先探讨数字图像水印能够实现的功能与相关应用场景. 值得注意的是, 数字图像水印虽能够实现多种功能, 但这些功能本质上都是由水印的鲁棒性和脆弱性扩展而来的. 因此, 可以将数字图像水印功能归纳为基于鲁棒水印技术和基于脆弱/半脆弱水印技术实现的 2 类功能.

2.1 基于鲁棒水印技术实现的功能

2.1.1 版权保护与所有权认证

载体图像的版权保护与所有权认证功能通过将包含图像版权信息、所有权信息的鲁棒水印隐藏至载体图像实现. 当图像存在版权、所有权争议时, 提取隐藏的水印即可证明真实的版权、所有权归属.

2.1.2 隐蔽通信

数字水印作为信息隐藏技术之一, 能够将保密/敏感数据以鲁棒水印的方式嵌入在普通载体图像. 嵌入水印对不可见性有要求, 因此, 他人难以发现图像中存在其他信息, 从而通过传输含水印的图像实现隐蔽通信. 同时, 鲁棒性保证了嵌入保密数据的可靠性与稳定性.

2.1.3 复制控制

在保护图像原创性和防止未授权复制方面, 数字图像水印技术可以提供一种简单的解决方案. 具体而言, 通过在图像中鲁棒地嵌入表示其复制状态, 如允许拷贝、禁止拷贝的特定水印信息实现. 当硬件或软件执行拷贝操作时, 版权管理系统会检测该状态并做出相应提示, 从而有效控制图像的复制行为[20].

2.1.4 源追踪

在图像分发前, 发送者可以将一次合法传播中接收者的标志信息(指纹)鲁棒地嵌入数字图像, 并将带有标志信息的副本传输给接收者. 若后期图像被未经授权的人分发, 可以通过提取水印(指纹)定位非法分发者, 实现源追踪.

2.2 基于脆弱/半脆弱水印技术实现的功能

2.2.1 内容认证和完整性验证

数字图像在传播中易被修改, 因此, 在需要保证图像完整性与真实性场景中, 使用前必须确定其完整性. 此时, 可通过嵌入脆弱水印鉴别. 核心思想是通过观察水印提取前后是否发生变化反映图像是否被修改. 若允许图像经受 JPEG 压缩等非内容修改, 则可通过嵌入半脆弱水印实现内容认证.

2.2.2 图像篡改定位(提示)

有时, 不仅需要检测图像篡改情况, 还需确定篡改区域位置, 以便接收方决定是否需要重传图像. 将载体图像划分为多个独立子块, 并为每个小块嵌入脆弱/半脆弱水印是常用的方法[21]. 提取时, 比较各子块水印变化去判定篡改情况, 整合所有篡改情况给出相应提示就能够定位篡改区域.

最近, Lefèvre 等[123]提出了一种基于 DWT 域量化嵌入的半脆弱水印算法. 该算法在解决篡改定位问题时引入错误定位码替代传统纠错码, 在实现精确篡改定位的同时降低了计算成本.

2.2.3 图像篡改区域恢复

图像篡改区域恢复功能指具备定位篡改区域并恢复该区域的能力. 该功能使得篡改图像能够继续使用, 无需重传. 基于自嵌入模式或块截断编码技术实现的脆弱/半脆弱水印往往具备该功能[124].

2.3 应用场景

2.3.1 数字作品知识产权保护领域

数字图像作为传统数字化作品, 其著作人享有发表、署名、修改、保护作品完整、复制等权利, 并且拥有许可他人以上述方式使用作品的权利. 因此, 在图像知识产权保护领域, 需要从版权、复制控制、完整性等多个维度进行保护. 通常, 鲁棒地嵌入相关著作人信息、授权信息等即可实现数字图像作品的保护. 数字图像具有可打印和易盗摄的特点, 若在图像印刷或重摄后仍能提取嵌入的水印, 则可实现更高级别的保护. Zhang 等[125]针对打印-重摄攻击提出一种鲁棒盲水印算法, 在图像 CIE Lab 颜色空间的 2 个颜色通道嵌入周期性水印, 并采用自卷积的方式实现几何校正, 提高了水印提取的准确性. 近年来, 深度学习模型作为新型数字作品, Li 等[126]通过嵌入水印妥善保护其版权.

2.3.2 电子商务/政务领域

在电子商务和电子政务领域, 用户在使用相关应用时, 需要将身份证、护照等重要证件和各种纸质票据的扫描图像上传至业务中心进行处理. 若图像在传输过程中被篡改, 可能会影响后续操

作, 因此, 可以在发送前嵌入脆弱/半脆弱水印, 服务端验证水印后决定图像是否需要重传. 此外, 在业务中心为用户生成电子证件/票据的应用场景中, 可以在生成的图像中鲁棒地隐藏认证标志, 以提高凭证的伪造难度.

2.3.3　军事通信领域

为了保护机密数据在传输中不被敌方探查, 军事通信系统可以利用无关图像等多媒体信息作为载体, 将机密信息作为水印鲁棒地嵌入载体后再传输, 实现隐蔽通信. 同时, 将脆弱水印嵌入载体, 可以通过监测图像篡改情况反映隐藏信息的可靠性. 此外, 若需要在军事图像中添加水印以证明其真实性和完整性或嵌入重要标记时, 需结合可逆或零水印技术实现, 以确保军事图像内容的精确性.

2.3.4　司法取证领域

数字影像技术广泛应用于司法取证, 但随着图像编辑软件的发展, 恶意用户可以轻松操作图像以伪造证据. 因此, 验证图像来源、真实性和完整性对于确保图像证据的可靠性至关重要. 数字图像水印是一种主动取证技术, 通过在图像数据生成或分发前嵌入源信息, 在必要时确定证据的来源和时间, 并通过嵌入(半)脆弱水印确定图像证据是否被篡改. 尽管水印提供了简单的实现方案, 但李晓龙等[127]认为检测图像操作痕迹进行鉴别的被动盲取证手段具有更小的使用限制, 更适合应用于取证领域.

目前, 网络中传输的图像多为 JPEG 格式, 因此, Rao 等[128]提出了一种适用于司法取证领域的抗 JPEG 压缩图像伪造检测和定位技术. 该算法采用了自监督域自适应网络, 由骨干网络和压缩逼近网络组成, 训练后得到了一个能够有效抵抗 JPEG 压缩并具有高精度定位能力的模型. 牛亚坤等[129]详细地对 JPEG 图像被动取证技术进行总结. 此外, 随着深度伪造技术的不断发展, 传统方法已无法察觉伪造痕迹, 基于深度学习的伪造检测技术已成为图像伪造检测的新方向. 周琳娜等[130]对近年基于人工智能的多媒体取证技术及取证领域目前常用的视觉深度伪造检测技术[131]进行了全面的梳理.

2.3.5　医学图像领域

数字图像水印技术在远程医疗领域得到广泛应用. 其一, 医学诊断图像是医疗诊断过程中的关键参考, 网络传输后, 为保证其真实性与完整性, 在诊断前必须进行确认, 否则会导致医生误诊. 因此, 通过嵌入脆弱水印可捕捉诊断图像的任意微小篡改. 另一方面, Fares 等[132]基于 DCT-Schur 分解和 DWT-Schur 分解将患者信息(电子病历)鲁棒地隐藏在医学图像, 在实现患者信息与诊断信息永久绑定的同时, 保护了患者隐私. 为了避免嵌入水印影响医学图像质量, 感兴趣区域(region of interest, ROI)[133]无损水印、可逆水印、零水印成为医学图像水印方案的首选.

3　数字图像多功能水印工作分类

数字图像多功能水印算法通过在同一载体嵌入不同类型的水印来实现多功能, 多数算法结合鲁棒水印与(半)脆弱水印进行设计. 根据多水印嵌入方式的不同, 多功能水印算法可归纳为 4 种模型: 融合水印嵌入模型、零水印嵌入模型、水印串行嵌入模型、水印并行嵌入模型. 本节对这 4 种模型进行介绍, 整理与分析各模型下经典的和近 10 年的水印算法.

3.1　融合水印嵌入模型

图 4 所示为融合水印嵌入模型的实现思路, 将多个水印通过复杂融合[134]或简单拼接[86,135]为单水印, 而后使用传统的单水印算法完成嵌入, 提取水印后还原为多个水印实现多功能. 显然, 这种模型可视作传统单水印的简单扩展, 算法设计的关键在于多水印的融合与还原.

Sharkas 等[134]较早提出了使用这一模式的多功能图像水印算法. 该方法将伪随机噪声序列作为水印 1, 加性融合在版权水印 2 执行 2 级 DWT

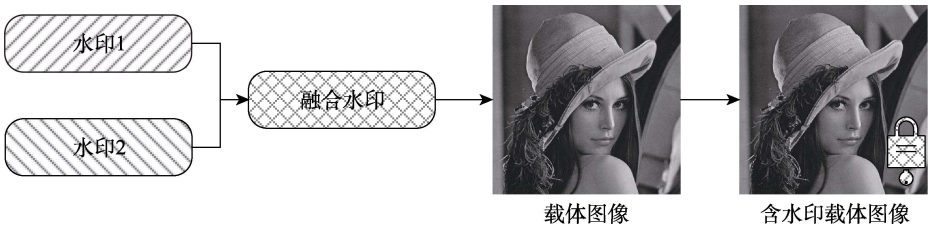


图 4　融合水印嵌入模型示意图

的系数 HL_2 中，得到融合水印. 将融合后的水印线性融合在载体图像 HL_2 和 HH_2 中完成嵌入. 该融合水印能够抵抗常见压缩、噪声、滤波攻击，可证明载体图像的版权. 提取的融合水印与原融合水印互相关，可以根据峰值检测水印 1 的存在. 当载体图像受到攻击后，对应的互相关峰值发生改变，证明图像遭受篡改. 该算法为非盲提取，版权图像水印的鲁棒性一般，并且只能粗略地检测篡改，但为多功能图像水印算法的实现提供了新思路.

Liu 等[135]提出了一种医学图像多功能水印算法，实现了版权认证、ROI 篡改检测、定位与恢复功能. 该算法将代表版权信息的医院标志和载体图像的 ROI 进行哈希处理，生成版权水印和篡改检测水印；同时，对医学图像 ROI 进行分块，并计算每区块的循环冗余校验码，产生篡改定位水印；最后，对每块 IWT 后低频系数进行块截断编码，生成对应的恢复信息. 将 4 种水印简单拼接为大水印，采用递归抖动调制方法，嵌入在载体图像 SLT 后低频系数 SVD 的矩阵. 该算法能够实现丰富的功能，嵌入水印具有较好的鲁棒性，并且在嵌入大容量信息后仍能保证载体图像质量，是较为优秀的图像多功能水印算法之一. 不足之处是版权水印为哈希值，在水印提取端不能直接根据水印内容确定版权归属.

Swaraja 等[86]与 Liu 等[135]提出的思路相似，将电子病历作为版权水印，与经过伦佩尔-齐夫-韦尔奇(Lempel-Ziv-Welch, LZW)无损压缩后 ROI 的亮度信息(作为恢复水印)简单拼接，并嵌入在载体图像亮度通道非感兴趣区域(region of non-interest, RONI)进行 DWT 后 HL_2，LH_2 区域分块 Schur 分解的矩阵中. 该水印的鲁棒性尚可，为了提高不可见性，采用粒子群细菌觅食优化(particle swarm bacterial foraging optimization, PSBFO)算法优化水印嵌入强度. 但篡改验证通过比较发送端与接收端载体图像 ROI 的哈希值证明，无法实现篡改区域定位，此外，恢复载体时需要额外提供 ROI 的色度信息.

基于融合水印嵌入模型的图像多功能水印算法本质上与单水印算法相同，最终只将单个水印嵌入载体图像. 不同之处在于，该类算法需要解决融合多种水印产生的问题. 若简单地将多水印拼接嵌入会导致嵌入数据量过大，从而降低载体质量；此外，攻击者可通过破解内嵌的单个水印破坏图像的所有保护措施；且算法需要原载体图像、水印或第三方机构的辅助才能同时实现版权验证、篡改检测等多种功能，过于依赖外界而非算法本身. 因此，大多数多功能水印算法未选择此模型. 近年来，融合模型集中应用在脆弱、半脆弱水印算法，在实现篡改定位和恢复上有着不错的效果[136-138]. 表 2 所示为融合水印嵌入模型算法的多功能实现与效果总结，尤其点明了多水印融合方式. 同时，表 3 对算法使用的技术与优缺点进行对比总结，可见，早期多功能水印算法存在明显缺点.

3.2 零水印嵌入模型

为了在设计多功能图像水印算法时能够直接应用传统单水印模型，同时保证水印嵌入后的载体质量，基于零水印模型的算法被提出. 图 5 所示为零水印嵌入模型的实现思路，将一种水印设置为零水印，在第三方机构的帮助下实现相关功能，另一水印按相应单水印算法完成嵌入.

Tarhouni 等[139]提出一种彩色图像版权验证和内容篡改检测的水印算法. 水印信息根据 *Y* 通道的纹理特征和 *Cb*，*Cr* 通道的色彩特征生成，具有

表 2 融合水印嵌入模型算法实现功能与效果总结

文献	版权保护	篡改检测/定位/恢复	多水印融合方式	鲁棒水印提取	(半)脆弱水印提取	载体/版权图像
[134]	是	是/否/否	复杂融合	非盲提取	非盲提取	灰度/灰度
[135]	是	是/是/是(ROI)	简单拼接	盲提取	盲提取	灰度/二值
[86]	是	是/否/是(ROI)	简单拼接	盲提取	盲提取	彩色(灰度)/灰度

表 3 融合水印嵌入模型算法使用技术与优缺点总结

文献	嵌入域	嵌入方法	优化方法	加密	优点	缺点
[134]	DWT	加性融合	无	无	提出融合水印思想	性能一般
[135]	SLT+SVD	量化	无	无	不可见性较高；实现较为精准的 ROI 恢复	版权水印为哈希值，不能直接根据内容确定版权归属
[86]	DWT+Schur	关系	PSBFO, LZW 无损压缩	无	水印嵌入容量大	恢复 ROI 时需要额外提供色度信息；未实现篡改定位

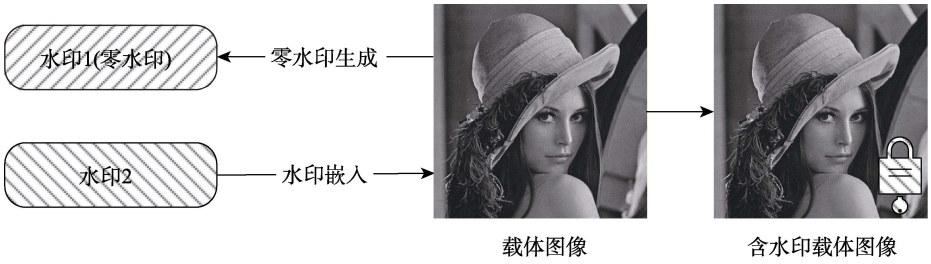


图 5　零水印嵌入模型示意图

唯一性. 生成后, 原创者将水印在权威机构注册, 用于后续版权证明. 同时也将水印嵌入在载体图像 Y 和 Cb 通道分块后部分子块 DCT 中频系数的 LSB, 完成半脆弱水印嵌入. 水印提取时, 首先进行 SURF 几何校正, 随后根据载体图像特征再次生成水印, 与从 LSB 提取的水印进行比对, 若两者 $\mathrm{BER} > 0.2$, 则认为载体图像内容遭到篡改. 将再次生成的水印与权威机构注册的水印信息进行匹配, 可查明图像版权. 算法使用零水印实现版权验证, 嵌入水印信息少所以不可见性较好, 但未实现篡改定位.

叶天语[140-141]提出了基于零水印模型的自嵌入双功能盲水印算法. 在自嵌入双功能模型中[140], 载体图像被分成子块, 特征水印根据各子块奇异值范数最高位奇偶性构造, 并嵌入在对应区块每个像素的最低 m 位. 鲁棒零水印则由所有区块产生的特征水印组成. 提取时, 根据图像特征水印与各子块最低 m 位水印的一致性实现篡改检测与定位. 在子块区域分割模型[141], 对分块后的每个子块进行 DCT, 并将得到的系数分为互不重叠的 2 个区域, 根据区域 1 奇异值均值最高位数字的奇偶性生成特征水印信息, 通过调整区域 2 中 2 个交流系数的大小完成水印嵌入. 提取时, 根据区域 1 重新生成特征水印与从区域 2 提取水印的一致性实现篡改检测与定位. 上述方法图像版权的鉴别通过计算重新生成的特征水印与第三方机构注册水印的归一化相关度实现. 朱光等[142]提出的多功能水印算法与上述算法相似, 不同的是针对彩色图像而设计. 其中, 特征零水印基于载体图像 SURF 特征生成, 该特征更为鲁棒. 内容认证则通过在图像空域 LSB 上嵌入脆弱水印实现.

上述算法的版权保护通过零水印机制实现, 但版权保护的水印信息根据图像特征生成, 是无实际意义的二值序列, 对图像所有者的体现不直观. 赵春晖等[143]为了改善这种情况, 将能够直接体现版权归属的标志作为鲁棒水印加性融合入载体图像 SVD 后的奇异值矩阵, 提取时可直接根据水印信息验明版权归属. 此外, 从鲁棒水印的密钥中抽取出一部分形成观测矩阵, 使用该观测矩阵对图像进行分块压缩感知, 观测值作为半脆弱水印注册、保存在第三方机构. 提取时重新计算半脆弱水印, 与存储的水印信息进行比对, 不一致则判断为篡改, 并且根据注册的零水印恢复载体图像. 除此之外, 赵彦霞等[144]将鲁棒水印与半脆弱水印均设置为零水印, 在不嵌入任何信息的情况下实现了彩色图像的版权保护和内容认证.

基于零水印和融合水印嵌入模型的多功能图像水印算法只需嵌入一次即可实现多种功能. 不同的是, 零水印方案嵌入的信息更少, 具有更好的不可见性, 而且水印之间无干扰, 破坏一个水印后, 另一个水印的功能尚可完成. 但此类算法仍存在不足: 多功能的实现需要可信第三方参与, 若第三方机构受到攻击或变得不可靠时会带来版权纠纷. 虽然区块链技术可以改善这种情况[145-146], 但多数多功能水印算法集中在稍后介绍的 2 种模型. 表 4 所示为零水印嵌入模型算法的多功能实现与效果总结, 特别强调了零水印的设置情况. 表 4 内容显示, 将版权水印设置为零水印的情况更为普遍, 只因版权水印通常携带了大量信息, 成为影响载体图像质量的要素之一. 表 5 所示为各算法使用的技术与优缺点.

3.3　水印串行嵌入模型

图 6 所示为水印串行嵌入模型的实现思路: 将实现不同功能的多个水印顺序嵌入载体图像. 基于此模型的算法要求后嵌入水印尽量不对前嵌入水印造成影响. 因此, 根据(半)脆弱水印易被改变和鲁棒水印难被破坏的特点, 通常先将版权信息鲁棒地嵌入, 再为包含鲁棒水印的载体图像嵌入(半)脆弱水印, 实现载体图像的篡改检测、定位、恢复. 该设计在最大程度上屏蔽了模型自身缺陷.

吕建平等[147]提出了基于混沌理论和量化的双功能图像水印算法. 鲁棒水印经过 Logistic 混沌序列置乱加密, 随之嵌入在载体 DWT 后的 LL_2 系数. 每个水印信息位采用均值量化的方法嵌入在 LL_2

表 4 零水印嵌入模型算法实现功能与效果总结

文献	版权保护	篡改检测/定位/恢复	零水印设置	鲁棒水印提取	(半)脆弱水印提取	载体/版权图像
[139]	是	是/否/否	版权水印	不提取	盲提取	彩色/零水印
[140]	是	是/是/否	版权水印	不提取	盲提取	灰度/零水印
[141]	是	是/是/否	版权水印	不提取	盲提取	灰度/零水印
[142]	是	是/是/否	版权水印	不提取	盲提取	彩色/零水印
[143]	是	是/是/是	认证水印	非盲提取	不提取	灰度/二值
[144]	是	是/是/否	均为零水印	不提取	不提取	彩色/二值

表 5 零水印嵌入模型算法使用技术与优缺点总结

文献	嵌入域	嵌入方法	优化方法	加密	优点	缺点
[139]	−/DCT	−/LSB	无	无	鲁棒水印抵抗几何攻击能力强; 不可见性高	未实现篡改定位
[140]	−/空域	−/LSB	无	无	不可见性高	版权认证需要原鲁棒特征水印
[141]	−/DCT	−/关系	无	Logistic	能够区分恶意/无意篡改	篡改定位精度不高
[142]	−/空域	−/LSB	无	Arnold	不可见性高; 篡改定位精度高; 版权零水印鲁棒性较高	版权保护需要第三方机构协助
[143]	SVD/−	加性融合/−	无	无	鲁棒与半脆弱水印互相补充	篡改检测与恢复步骤较复杂
[144]	−/−	−/−	无	Arnold	不可见性高(不嵌入水印)	篡改定位精度不高

注. −表示不考虑嵌入操作.

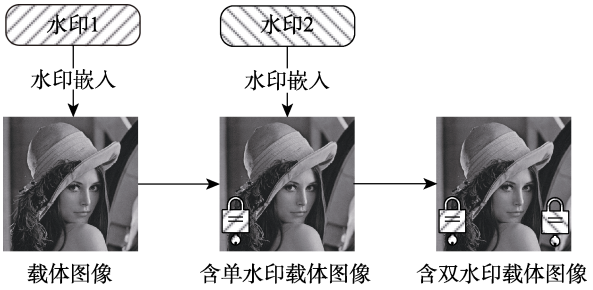


图 6 水印串行嵌入模型示意图

系数的 4×4 区块中. 区块量化步长自适应于其能量与纹理特征, 以平衡水印的鲁棒性和不可见性. 图像变换回空域后, 根据特征自生成脆弱水印, 嵌入在 LSB. 算法中, 鲁棒水印抵抗信号处理攻击能力较好, 脆弱水印可以实现 8×8 精度的篡改检测和定位, 而且实现了双水印的盲提取, 但未说明双水印嵌入后的不可见性.

Kunhu 等[148]与吕建平等[147]提出的模式相似, 采用奇偶量化的方法嵌入版权水印. 并在 RGB 空间将每个色彩通道分为 32×32 的区块, 取区块内一半像素的哈希值作为脆弱水印, 嵌入其余像素的 LSB. 此算法版权水印具有一定的鲁棒性, 而且实现了双水印的盲提取, 不足之处是版权水印未加密, 缺乏安全性, 而且篡改检测精度不高.

上述算法在频域基于量化方法嵌入鲁棒水印, 基于空域 LSB 嵌入脆弱水印, 能够实现双水印的盲提取. 但鲁棒水印只能抵抗基础的信号处理攻击, 对旋转、缩放等几何攻击没有很好的应对措施, 因此, 部分工作将 SVD 应用在多功能水印算法, 利用 SVD 的几何不变性提高版权水印的鲁棒性[118,149-150].

Ansari 等[149]将版权鲁棒水印加性嵌入在 SVD 后的奇异值矩阵, 设计基于图像相关性的目标函数并使用 PSO 优化算法确定水印嵌入强度. 之后, 载体图像分为 4×4 大小的区块, 进行 Arnold 置乱, 每块根据矩阵的迹构造 10 bit 区块验证码, 根据连续 5 个区块验证码的均值构造 6 bit 组验证码, 结合生成特征信息. 将特征信息与 Logistic 生成的混沌随机序列和脆弱水印中的 16 bit 信息重构为 16 bit 信息后嵌入所在区域 LSB. 提取时, 通过区块、组验证码进行双重验证, 提高篡改检测与定位的精度. 最终, 水印鲁棒性得到提高, 但整体基于空域嵌入, 鲁棒性不足且未实现盲提取.

2017 年, Ansari 等[118]提出将鲁棒水印的主成分加性融合在载体图像 LL_3 系数进行 SVD 的奇异值矩阵. 为了提高水印的不可见性, 使用 ABC 优化算法计算较优的嵌入强度. 鲁棒水印嵌入后, 将载体图像恢复到空域, 分为 4×4 大小的区块, 根据各区块奇异值构造脆弱水印. 区块进一步划分为 2×2 大小的子区块, 取子区块系数均值的前 5 个有效位作为该区块的恢复信息. 最终, 脆弱水印嵌入在本区块最低与次低有效位, 提取时和重新生成的脆弱水印比对, 判断是否篡改. 恢复水印嵌入在映射区块的最低与次低有效位, 必要时可提取并修复图像. 算法实现了灰度图像的版权保护、篡改定位、篡改恢复, 水印嵌入的容量较大. 但鲁

棒水印属于非盲提取, 用来恢复图像的水印本身嵌入在空域, 易被修改, 不能提供可靠的恢复.

陈善学等[150]提出的彩色图像多功能水印算法使用多变换域提高版权水印的鲁棒性, 引入四元数提高透明度. 首先, 将载体图像分通道进行 DWT, 对中低频系数进行四元数离散余弦变换 (quaternion discrete cosine transform, QDCT)后选取实数矩阵的部分元素构造与鲁棒水印尺寸相同的新矩阵, 并将鲁棒水印加性嵌入在新矩阵 SVD 的系数. 恢复图像到空域后再次进行 QDCT, 根据低频系数构造脆弱水印并嵌入在所有颜色通道的 LSB. 实验结果表明鲁棒水印能够抵抗多种攻击, 脆弱水印能够实现较为精准的篡改定位, 但鲁棒水印仍是非盲提取.

上述工作基于加性嵌入, 提取信息时需要原载体图像的参与, 为非盲提取方法. 许多工作探索性能更好的多功能图像水印盲提取算法[87,151-152].

Liu 等[151]提出的双盲提取彩色图像多功能水印算法将灰色鲁棒水印嵌入在载体图像 YCbCr 颜色空间的亮度通道: 首先, 对 Y 通道进行 DWT, 取 LL 系数复制在新矩阵; 将新矩阵分为 8×8 大小的区块, 每个区块量化后, 将鲁棒水印加性嵌入其中, 对所有区块完成操作后替换原 HH 系数. 水印提取时, 参考的矩阵由接收图像 LL 系数生成, 无需额外提供载体信息, 实现了盲提取. 脆弱水印采用改进的 LSB 方法, 能够精准地检测与定位篡改区域. 此算法鲁棒水印有抵抗噪声、JPEG 压缩、亮度变化等基础攻击的能力, 但由于嵌入在 HH 区域, 鲁棒性仍有提升空间.

Ahmadi 等[152]也针对彩色载体图像设计出双盲提取水印算法. 该算法使用视觉熵和边缘熵选出修改后不易察觉的亮度高、纹理复杂区域, 并记录位置; 后取载体图像蓝色通道 LL 系数进行 4×4 分块, 根据记录选定对应位置作为嵌入区块; 对各区块进行 SVD, 根据水印信息修改 2 对相似系数 $U(2,1)$ 和 $U(3,1)$, 以及 $V(2,1)$ 和 $V(3,1)$ 的大小关系, 完成 2 bit 信息的嵌入. 为提高水印不可见性, 使用 PSO 优化嵌入强度 T_1 和 T_2. 脆弱水印则嵌入在所有颜色通道 DWT 后 HH 系数分块 SVD 后的 $\boldsymbol{S}$ 矩阵中. 水印提取时基于相位相关性(phase correlation, PC)进行几何校正, 以提高鲁棒水印抵抗几何攻击的能力. 实验结果表明, 算法基于 HVS 特性与优化理论的确提高了水印的不可见性, PSNR 经常维持在 45 dB 之上, 且鲁棒水印抵抗各种攻击能力强.

Koley[87]提出了双盲提取的灰度图像双功能水印方案. 鲁棒水印嵌入在载体图像使用扩展的量子切割算法[153](extended quantum cuts, EQCUT)提取的显著区域. EQCUT 是一种显著性目标分割算法, 通过增加超像素抽象和改善图像连通性等能力, 能够准确地分割出包含显著内容且与周围背景良好分离的视觉显著区域. 由于视觉显著区域具有丰富的特征, 将水印嵌入该区域比在图像平滑区域进行修改更难以被 HVS 感知, 从而确保了水印嵌入后的不可见性. 算法采用调整系数大小关系的方法将 Arnold 置乱的鲁棒水印嵌入在显著区域 Hessenberg 分解后的矩阵中, 脆弱水印嵌入在载体 LL_2 系数的 LSB. 实验证明该算法具有较高的不可见性, PSNR 可以维持在 45 dB 之上.

上述算法实现了双水印的盲提取, 适合部署于真实应用场景. 其中, 远程医疗是数字图像水印技术重要的应用领域, 部分工作探索了基于串行嵌入模型的医学图像多功能水印算法[88,154-155].

ROI 指包含诊断信息(器官、骨骼等)的关键区域, RONI 则是非关键区域. 由于整幅图像的无损修复较困难, 大部分算法着眼于 ROI 的无损恢复. Alshanbari[154]提出了应用在灰度医学图像的多功能水印算法, 可实现所有权保护、篡改检测和恢复功能. 该算法对 ROI 和 RONI 进行分割, 并将灰度鲁棒水印的主成分加性嵌入在载体 LL_3 系数 SVD 后的奇异值矩阵中. 之后, 使用 LZW 算法对 ROI 无损压缩, 生成恢复水印. 同时, 对 ROI 哈希产生篡改检测水印, 与恢复水印嵌入在 RONI 的 LSB. 提取时, 首先生成图像 ROI 的哈希值, 与提取的篡改检测水印进行比对, 若判断为篡改则使用修复水印无损恢复 ROI, 最后提取鲁棒水印证明所有权. 算法虽然能够实现 3 种功能, 但恢复水印和篡改检测水印易被破坏, 难以保证篡改检测与图像恢复的正确性.

Sinhal 等[155]提出了一种医学图像的多功能水印算法, 与其他算法不同, 该算法关注了 RONI 的篡改情况. 首先, 将鲁棒二值水印以基于关系的方式嵌入 SLT 频域. 图像恢复到空域后, 使用 LZW 算法对 ROI 进行无损压缩, 生成修复水印. 再将 RONI 分为 8 块, 求每块和 ROI 的哈希值作为篡改检测水印, 与修复水印结合、置乱后嵌入在 RONI 任意区块的 LSB. 提取时, 根据每区块哈希值定位篡改区域, 若 ROI 篡改, 则进行无损恢复, 最后提取鲁棒水印进行所有权认证. 实验结果表明, 该算法水印鲁棒性较强, 恢复水印和篡改检测水印结合 RONI 区域篡改检测与随机置乱, 可靠性较

Alshanbari[154]的工作有所提高, 而且实现了水印的双盲提取. 但嵌入双水印后的不可见性仍可提升, 修复水印也需更加鲁棒.

Sinhal 等[88]基于 IWT、调整 HL 和 LH 子带均值大小嵌入方法、九进制修正的 LSB 算法实现对载体图像的所有权验证、篡改检测与定位、全域篡改恢复, 能够满足医学图像的保护要求.

表 6 所示为水印串行嵌入模型算法的多功能实现与效果总结. 表 7 对各算法使用的技术与优缺点进行了总结.

表 6 水印串行嵌入模型算法实现功能与效果总结

文献	版权保护	篡改检测/定位/恢复	鲁棒水印提取	(半)脆弱水印提取	载体/版权图像
[147]	是	是/是/否	盲提取	盲提取	灰度/二值
[148]	是	是/是/否	盲提取	盲提取	彩色/二值
[149]	是	是/是/否	非盲提取	盲提取	灰度/灰度
[118]	是	是/是/是	非盲提取	盲提取	灰度/灰度
[150]	是	是/是/否	非盲提取	盲提取	彩色/二值
[151]	是	是/是/否	盲提取	盲提取	彩色/灰度
[152]	是	是/是/否	盲提取	盲提取	彩色/二值
[87]	是	是/是/否	盲提取	盲提取	灰度/二值
[154]	是	是/否/是(ROI)	非盲提取	盲提取	灰度/灰度
[155]	是	是/是/是(ROI)	盲提取	盲提取	灰度/二值
[88]	是	是/是/是	盲提取	盲提取	灰度/二值

表 7 水印串行嵌入模型算法使用技术与优缺点总结

文献	嵌入域	嵌入方法	优化方法	加密	优点	缺点
[147]	DWT/空域	量化/LSB	无	Logistic	篡改定位精度较高	未说明水印的不可见性
[148]	DWT/空域	量化/LSB	无	无	鲁棒水印能够抵抗轻微的几何攻击	篡改定位精度不高
[149]	SVD/空域	加性融合/LSB	PSO	无	水印嵌入容量大; 篡改定位精度较高	鲁棒水印非盲提取; 未明显提高抵抗几何攻击能力
[118]	DWT+SVD/空域	加性融合/LSB	ABC	无	水印嵌入容量大; 实现 3 种功能	鲁棒水印非盲提取; 恢复信息嵌入空域, 不能提供可靠恢复
[150]	DWT+QDCT+SVD/空域	加性融合/LSB	无	Logistic	不可见性高; 鲁棒水印能够抵抗旋转与剪切攻击; 篡改定位精度高	鲁棒水印非盲提取
[151]	DWT/空域	加性融合/修正 LSB	无	无	水印嵌入容量大; 篡改定位精度高; 不可见性较好	鲁棒性需要提升
[152]	DWT+SVD/DWT+SVD	关系/关系	PSO, PC 几何校正	Arnold	不可见性极高; 鲁棒水印抵抗几何和混合攻击效果好; 篡改定位精度高	鲁棒水印抵抗高强度椒盐噪声攻击与 JPEG 压缩效果一般
[87]	Hessenberg/DWT	关系/LSB	EQCUT	Arnold	不可见性高; 篡改定位精度高	鲁棒水印抵抗高强度攻击能力不足
[154]	DWT+SVD/空域	加性融合/LSB	LZW 无损压缩	无	不可见性高; ROI 100%恢复	鲁棒性欠佳且非盲提取; 未实现篡改定位
[155]	SLT/空域	关系/LSB	LZW 无损压缩	无	水印嵌入容量大; 不可见性较高; ROI 100%恢复	篡改定位精度不高; 鲁棒水印抗几何攻击能力不足
[88]	IWT/空域	关系/修正 LSB	无	Arnold	不可见性较高; 篡改定位精度高且恢复能力强	水印嵌入容量小; 鲁棒水印抗几何攻击能力不足

3.4 水印并行嵌入模型

图 7 所示为水印并行嵌入模型的实现思路: 将实现不同功能的多个水印同时嵌入在载体图像的不重叠区域(不同空间位置、不同颜色通道、不同频率分量). 此类算法最大优势是嵌入的多个水印互不干扰, 能够减少前类算法中后嵌入水印对前嵌

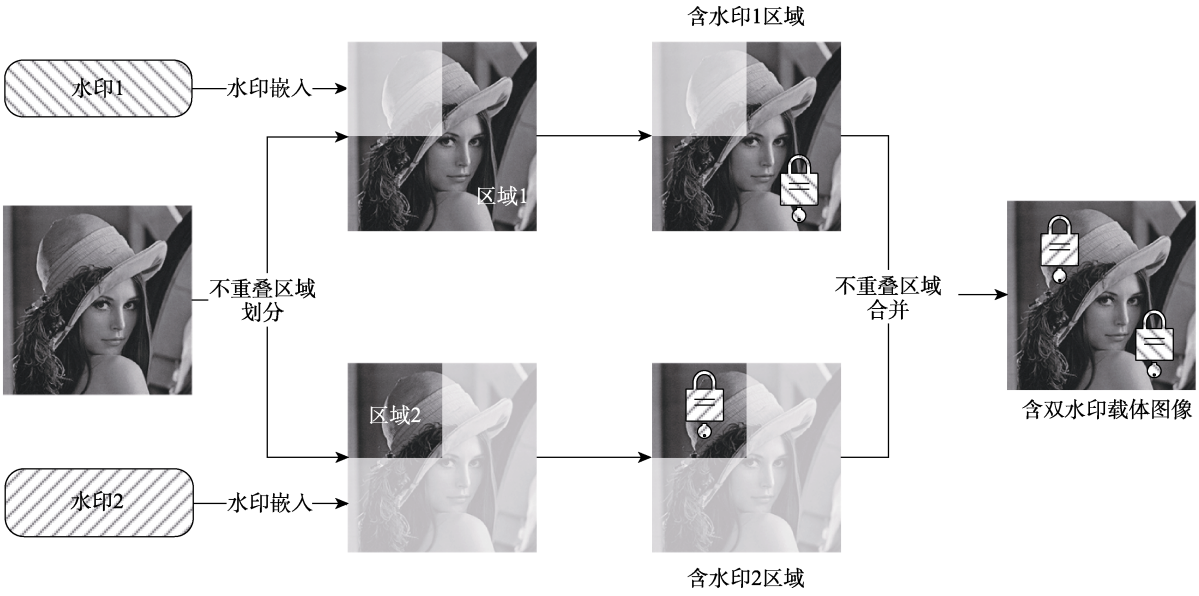


图 7　水印并行嵌入模型示意图

入水印的影响. 此外, 多水印独立嵌入, 选择好水印各自嵌入区域后就可以并行执行相应单水印方法, 因此, 该模型的扩展度更强. 目前, 多数多功能图像水印算法选择并行嵌入模型.

Shen 等[156]提出嵌入在 DWT 系数不同区域的灰度图像多功能水印算法. 载体图像多级 DWT 后, 对细节子带分块, 并根据 HVS 特性进行区块排序. 将鲁棒水印嵌入前几个能量大、纹理复杂的区块, 人眼不易察觉. 脆弱水印则随机嵌入在余下区块的最低或次低有效位. 算法实现了多功能, 修改的 LSB 算法使脆弱水印安全性得到提高, 但水印不可见性一般, 鲁棒水印抵抗攻击时性能不佳且为非盲提取, 因此, 仍有较大提升空间.

Shi 等[157]对其优化. 载体图像经过 3 级 IWT 后划分为 5×5 区块, 为保证载体图像质量, 不修改 LL_3 范围的系数. 对剩余区块计算与 JPEG 压缩图像区块的 MSE, 根据 MSE 选出遭受修改后系数不易变区域作为鲁棒水印嵌入域, 余下则嵌入脆弱水印. 鲁棒水印采用状态编码技术嵌入, 实现了盲提取. 脆弱水印嵌入与 Shen 等[156]提出的相似, 并且在最终位替换时增加了补偿规则. 实验结果表明, 水印的不可见性有所提高, 鲁棒水印抵抗常见攻击的性能有提升, 但水印嵌入量有所减少, 而且脆弱水印实现篡改定位效果不够精确.

Lei 等[158]提出了一种将鲁棒水印和脆弱水印分别嵌入在 IWT 后不同区域的算法. 鲁棒二值水印和脆弱水印在嵌入前与切比雪夫映射生成的二值序列进行异或加密. 载体图像 IWT 后, 取 LL 系数分块执行 SVD, 并将鲁棒水印量化嵌入在奇异值矩阵中, 脆弱水印采取相同方法嵌入 HH 系数. 算法采用 ABC 智能算法计算较优量化步长, 改善水印不可见性. 实验表明, 鲁棒水印抵抗几何攻击的能力较好, 脆弱水印能够实现内容认证且双水印均为盲提取.

Haghighi 等[122]提出了基于 ST、多层感知机(multilayer perceptron, MLP)和 NSGA-II 多目标优化的彩色图像多功能水印算法, 多水印嵌入在图像亮度通道 ST 后的不同区域. 首先, 鲁棒水印与随机二值序列进行异或加密, 并使用 CCS 置乱, 随后生成随机二值序列作为半脆弱水印. 水印嵌入前, 算法基于纹理将区块分为粗糙或平滑块, 并使用 K-means 算法对块进行聚类, 得到几类不同粗糙程度的区块, 并给出相应纹理系数 ξ. 将载体图像转换到 YCoCg 颜色空间, 对亮度通道进行 ST, 得到近似子带和 6 个方向子带. 对子带进行 LWT, 取 LL 系数并执行分块 DCT, 鲁棒水印通过量化融合在近似子带 DCT 系数, 半脆弱水印通过关系嵌入在方向子带 DCT 系数, 嵌入时均使用对应纹理系数 ξ 调整强度. 量化步长与调整步长由 NSGA-II 多目标优化算法计算出较优值, 与 ξ 一起平衡水印嵌入的鲁棒性和不可见性. 最终, 通过 MLP 根据最大可能相关性提取半脆弱水印, 与原水印比对后定位篡改区域. 实验证明, 双水印嵌入后 PSNR 均值可达 42 dB, 鲁棒水印抵抗常见攻击能力强, 但抵抗几何攻击能力有待提高.

Al-Haj 等[159]与 Priyanka 等[160]基于医学图像

设计, 将脆弱水印嵌入在需要检测篡改的 ROI, 将鲁棒水印嵌入在 RONI, 实现多水印嵌入. 在 Al-Haj 等[159]提出的方法中, 给定的脆弱二值水印嵌入到 ROI 的 LSB, 并将原 LSB 信息作为鲁棒水印之一, 提取时负责将 ROI 恢复到原状态. 同时, 使用患者信息和版权图像作为另外 2 个鲁棒水印. 随后, 对 RONI 分块执行 DWT, 将三者分别嵌入在 LH, HL, HH 系数进行 SVD 后 $S(0,0)$ 系数的最低位. Priyanka 等[160]提出的模式与上述方法类似, 脆弱水印根据像素前 6 个有效位自生成, 嵌入在 ROI 后 2 个位平面. 鲁棒水印是病患信息、版权图像与原 2 个位平面信息. 对 RONI 分块执行 IWT, 将鲁棒水印分别嵌入在 LH, HL, HH 系数进行 SVD 后的 $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 矩阵中, 基于大小关系每区块完成 2 bit 信息嵌入. 2 个算法的鲁棒水印都能抵抗基础信号处理攻击, 但抵抗几何攻击效果不佳. 篡改检测与定位精度高且均实现了水印的盲提取, 后者的不可见性略高.

上述算法针对灰度图像设计, 水印间无干扰地嵌入单通道图像不同空间位置或不同频率分量, 并且很轻易推广至彩色载体图像. 但在一幅单通道图像中嵌入过多信息, 易使图像降质. 下述算法则将不同水印嵌在彩色图像的不同通道, 实现多功能的同时提高水印嵌入后的不可见性.

吴楠等[161]与虞晓庆等[162-163]提出的方法在实现彩色图像的版权保护和内容认证上具有相似模式, 均将版权水印嵌入在蓝色分量, 并根据绿色分量自生成认证水印, 嵌入绿色通道. 在自生成认证水印部分, 3 种算法对载体绿色分量进行 X 级 LWT 或 DWT, 求最高层低频系数 LL_X 的能量均值, 以均值为二分阈值, 生成由 0 与 1 组成的认证水印, 并进行 Arnold 置乱和异或加密. 虞晓庆等[162-163]提出的方法紧接着将认证水印量化在 HL_X 和 LH_X 中能量大的区域. 在吴楠等[161]提出的方法中, 绿色分量进行 Y 级 DWT, 取 LH_Y 系数并进行 4×4 分块, 提取每块 DCT 后的 $(1,1)$ 系数构造新矩阵再量化嵌入. 在鲁棒水印嵌入方面, 虞晓庆等[162]首先对版权水印扩频, 得到 4 个完全相同的水印 $\boldsymbol{W}_{11}$, $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{13}$, $\boldsymbol{W}_{14}$. 置乱后, 将 $\boldsymbol{W}_{11}$, $\boldsymbol{W}_{12}$ 嵌入在蓝色分量 Z 级 LWT 后 LH_Z 和 HL_Z 数值的第 4 位平面, 将 $\boldsymbol{W}_{13}$, $\boldsymbol{W}_{14}$ 基于关系嵌入 $\mathrm{LH}_{Z\text{-}1}$ 和 $\mathrm{HL}_{Z\text{-}1}$. 提取时, 4 个扩频水印互相补充, 能够恢复一个完整的版权水印. 虞晓庆等[163]提出的另一种方法对鲁棒二值水印加密后乘性嵌入在蓝色分量多级 LWT 的 LL_Z 部分位置, 嵌入位置与 HH_Z 区域的大系数坐标一致. 吴楠等[161]对鲁棒二值水印加密后量化嵌入在蓝色分量多级 DWT 后的 LL_Z 区域. 3 种算法鲁棒水印对噪声、滤波、JPEG 压缩有较好的抵抗力. 认证水印是半脆弱水印, 实现了载体图像内容篡改检测与大致定位. 其中, 虞晓庆等[162-163]提出的方法水印不可见性更优. 吴楠等[161]与虞晓庆等[162]提出的方法实现了双水印的盲提取.

蓝夏梅等[164]提出一种基于纠错编码的多功能水印算法, 鲁棒水印嵌入红色分量频域, 认证水印嵌入绿色分量空域. 首先, 对载体图像分块进行 DCT 后量化系数, 重新进行二进制编码. 将 3 个通道生成的编码连接后使用 $(7,4)$ 汉明码进行纠错编码, 生成 63 bit 二值序列, 加密后嵌入在 Torus 自同构变换映射区块绿色分量像素的后几个位平面, 完成认证水印的生成与嵌入. 提取时, 若区块重新生成的水印与映射块提取水印不相等, 则判为篡改, 根据提取水印恢复篡改区域. 鲁棒二值水印 Arnold 置乱后嵌入红色分量 DCT 的中频系数. 算法实现了双水印的盲提取, 脆弱水印能大致定位篡改区域并恢复, 但恢复信息基于空域嵌入, 易被破坏, 鲁棒水印只能抵抗简单攻击.

Sivananthamaitrey 等[165]提出一种针对彩色医学图像的多功能水印算法. 鲁棒水印是证明患者身份信息的灰度图像, SWT 后取细节频带 HH 进行 SVD, 将对应奇异值矩阵加性嵌入在载体绿色分量的 SWT-SVD 的奇异值矩阵中. 嵌入少量水印信息, 保证了载体图像的质量. 脆弱水印嵌入在载体蓝色通道的 LSB. 实验结果显示, 鲁棒水印抵抗多种攻击效果好, 但提取时需要大量的原载体与水印信息, 实用性不强. 脆弱水印只能实现 256×256 粒度的篡改定位, 检测虚警率高. 3 年后, Sivananthamaitrey 等[117]提出优化, 鲁棒水印嵌入强度通过 GA 求出. 实验结果表明, 嵌入双水印后不同载体图像的 PSNR 介于 37~54 dB, 不可见性确有提高. 鲁棒水印抵抗多类型攻击的效果好, 但仍是非盲提取, 且篡改定位的虚警率较高.

Hurrah 等[166]设计出双盲提取的彩色图像多功能水印方法. 该算法先对鲁棒水印进行 Arnold 置乱和原创加密算法双重加密, 保证其安全性. 之后, 取载体图像的蓝色通道进行 DWT 并对 LL 系数 8×8 分块, 每块分为 4 子块进行 DCT, 根据水印值将一对子块差值量化在不同区域完成鲁棒水印嵌入, 所有子块重复相同操作. 脆弱水印嵌入在载体绿色平面: 绿色通道图像分为 8×8 大小的区块后,

根据均值生成特征水印嵌入在系数 LSB. 算法嵌入双水印后的 PSNR 值大于 40 dB, 水印不可见性较高. 鲁棒水印能够抵抗一定程度的剪切和缩放攻击. 脆弱水印篡改检测精度优于 Sivananthamaitrey 等[117,165]提出的方案, 而且能够实现双水印的盲提取.

上述彩色图像多功能水印算法将不同水印嵌入在 RGB 颜色空间的不同通道时, 不需要进行色彩空间转换, 复杂性低, 但易使载体图像色彩发生偏差. Wan 等[28]认为将水印嵌入在图像的 YCbCr 颜色空间会更加鲁棒. Kumar 等[167]证明将水印嵌入在 YCbCr 颜色空间中的 *Y* 通道具有更好的不可见性. 因此, 基于 YCbCr 的水印算法在平衡鲁棒性和不可见性时有较好效果.

Zhao 等[168]提出将鲁棒水印嵌入载体 YCbCr 颜色空间的 *Cb* 通道, 对 *Cb* 通道执行 3 级 DWT, 取 LL_3, LH_3, HL_3 的每个系数构成三元组并将加密后的水印采用 DM 方法嵌入对应三元组. *Cr* 通道执行 8×8 分块的 DCT, 半脆弱水印通过 STDM 嵌入中频系数. 算法基本上可以实现版权保护和篡改检测、定位的双功能, 嵌入双水印后载体图像质量较好, 但鲁棒和半脆弱水印性能有待提高.

Kamili 等[169]提出了应用在工业物联网图像采集场景中的多功能水印算法, 强调了实时性. 对鲁棒水印进行 Logistic 混沌序列异或和 DNA 双重加密, 嵌入在载体图像 YCbCr 颜色空间的 *Y* 通道, 嵌入方法同 Hurrah 等[166]提出的方案. 脆弱水印嵌入在 *Cb* 通道空域, 利用四邻域预测像素值. 实验结果显示, 双水印对载体图像的影响较小, 嵌入后 PSNR 值在 40 dB 之上. 鲁棒水印抵抗混合攻击效果优异. 脆弱水印能够实现较为准确的篡改检测与定位. 算法能够实现盲提取且嵌入与提取时间短, 适合实时性要求高的场景.

表 8 所示为水印并行嵌入模型算法的多功能实现与效果总结, 尤其强调了不重叠区域的选择, 能够看出彩色图像更倾向于将水印嵌入 RGB 空间. 表 9 所示为各算法使用的技术与优缺点. 此类方法虽然灵活性强, 但多水印嵌入不重叠区域的面积越大, 对载体图像质量的影响就越大.

表 8　水印并行嵌入模型算法实现功能与效果总结

文献	版权保护	篡改检测/定位/恢复	不重叠区域选择	鲁棒水印提取	(半)脆弱水印提取	载体/版权图像
[156]	是	是/是/否	不同频率分量	非盲提取	盲提取	灰度/灰度
[157]	是	是/是/否	不同频率分量	盲提取	盲提取	灰度/灰度
[158]	是	是/是/否	不同频率分量	盲提取	盲提取	灰度/二值
[122]	是	是/是/否	不同频率分量	盲提取	盲提取	彩色(灰度)/二值
[159]	是	是/是/否	ROI 与 RONI	盲提取	盲提取	灰度/二值
[160]	是	是/是/是	ROI 与 RONI	盲提取	盲提取	彩色(灰度)/二值
[161]	是	是/是/否	RGB 不同通道	盲提取	盲提取	彩色/二值
[162]	是	是/是/否	RGB 不同通道	盲提取	盲提取	彩色/二值
[163]	是	是/是/否	RGB 不同通道	非盲提取	盲提取	彩色/二值
[164]	是	是/是/是	RGB 不同通道	盲提取	盲提取	彩色/二值
[165]	是	是/是/否	RGB 不同通道	非盲提取	盲提取	彩色/灰度
[117]	是	是/是/否	RGB 不同通道	非盲提取	盲提取	彩色/灰度
[166]	是	是/是/否	RGB 不同通道	盲提取	盲提取	彩色/二值
[168]	是	是/是/否	YCbCr 不同通道	盲提取	盲提取	彩色/二值
[169]	是	是/是/否	YCbCr 不同通道	盲提取	盲提取	彩色/二值

3.5　算法总结与分析

目前, 数字图像多功能水印算法均基于上述 4 种模型, 每类模型都旨在对现有单水印算法修改最少的情况下将不同单水印算法移植在载体图像上, 实现不同功能. 表 10 总结了 4 种模型的特点. 其中, 基于融合水印嵌入模型和零水印嵌入模型的算法本质上都最多执行一次水印嵌入过程, 与其他模型算法相比具有较低的时间复杂度. 但这 2 种模型在实现多功能时大多依赖可信第三方机构存储的信息, 因此, 研究人员设计算法时需要考虑存储成本与部署后的安全性. 基于水印串行、并行嵌入模型的算法虽然存在缺点, 但总体性能好、存储成本低. 目前, 基于串行、并行嵌入模型的多功能图像水印算法更为主流.

对表 2~表 9 所示的多功能水印算法实现的多种功能、嵌入域、嵌入方法以及优缺点进一步总结, 可将当前数字图像多功能水印算法的整体趋势归纳如下:

表 9 水印并行嵌入模型算法使用技术与优缺点总结

文献	嵌入域	嵌入方法	优化方法	加密	优点	缺点
[156]	DWT/DWT	加性融合/修正 LSB	无	无	改进的 LSB 提高安全性	鲁棒水印不能抵抗复杂攻击
[157]	IWT/IWT	状态编码/修正 LSB	无	无	水印嵌入容量大; LSB 补偿算法提高不可见性	篡改定位精度不高
[158]	IWT+SVD/IWT	量化/量化	ABC	切比雪夫映射	鲁棒水印抵抗多种攻击能力强	不可见性一般; 未对篡改检测与定位进行详细解释
[122]	ST+LWT+DCT/ST+LWT+DCT	量化/关系	NSGA-II, MLP, *K*-means	CCS 置乱	不可见性较高	算法复杂度高; 鲁棒水印抵抗几何攻击能力不足
[159]	DWT+SVD/空域	LSB/LSB	无	无	水印嵌入容量大	鲁棒性需要提升
[160]	IWT+SVD/空域	关系/LSB	无	无	不可见性高; ROI 嵌入水印后可恢复	鲁棒水印抵抗几何攻击效果一般
[161]	DWT/DWT+DCT	量化/量化	无	Logistic, Arnold	认证水印能够抵抗 JPEG 压缩	鲁棒性需要提升
[162]	LWT/LWT	LSB、关系/量化	无	Logistic, Arnold	水印嵌入容量大; 鲁棒水印抵抗剪切攻击效果较好	鲁棒水印实验不充分
[163]	LWT/LWT	乘性融合/量化	无	Hilbert, Logistic, Arnold	不可见性较高; 版权水印抵抗 JPEG 压缩效果较好	鲁棒水印仅能抵抗简单攻击
[164]	DCT/空域	关系/LSB	无	Arnold	实现篡改区域恢复	鲁棒水印仅能抵抗简单攻击
[165]	SWT+SVD/空域	加性融合/LSB	无	无	水印嵌入容量大	鲁棒水印非盲提取; 篡改定位虚警率高
[117]	SWT+SVD/空域	加性融合/LSB	GA	无	水印嵌入容量大; 不可见性高; 鲁棒性强	鲁棒水印非盲提取; 篡改定位虚警率高
[166]	DWT+DCT/空域	量化/LSB	无	Arnold 与自定义加密	不可见性较高; 鲁棒水印抵抗混合攻击能力强	篡改定位精度不高
[168]	DWT/DCT	量化/量化	无	Arnold	不可见性较高	鲁棒水印抵抗 JPEG 压缩与中值滤波效果不佳
[169]	DCT/空域	量化/预测误差扩展	无	Logistic, DNA	不可见性高; 鲁棒水印能够抵抗混合攻击; 实时性好	鲁棒水印抗几何攻击能力不足

表 10 多功能水印嵌入模型特点总结

多功能水印嵌入模型	描述	水印嵌入次数	优点	缺点	模型实现要点
融合水印嵌入模型	多种水印融合或连接为单水印后嵌入载体图像	1 次	简单性	攻击者破解内嵌的单水印后可打破所有的保护措施	融合/连接方法的选择
零水印嵌入模型	至多嵌入 1 种水印, 其他功能的水印设计为零水印	0 或 1 次	水印之间无干扰; 不可见性较好	多功能的实现需要可信第三方参与	零水印的生成与存储
水印串行嵌入模型	多种水印顺序嵌入载体图像	2 次	简单性	对水印嵌入顺序和方法有较高要求	多水印嵌入顺序
水印并行嵌入模型	多种水印嵌入在载体图像的不重叠区域	2 次及以上	多水印互不干扰, 可扩展性强	可能对载体图像质量带来较大影响	不重叠区域的划分与选择

(1) 从水印算法实现功能上看, 多数算法选择结合鲁棒水印与(半)脆弱水印的特点, 设计能够同时满足图像版权保护及所属认证、篡改检测与定位的双功能算法. 随着应用需求的增加, 图像篡改后

恢复也逐渐成为多水印算法考虑的第 3 种功能.

(2) 从水印算法的安全性来看, 多数算法加密水印以提高安全性. Arnold 置乱和 Logistic 混沌映射因简单高效成为备受欢迎的图像加密方法. 部分算法设计了独特的加密过程提高破解难度. 除加密外, 一些算法通过置乱水印嵌入块、随机选择水印嵌入块来提高系统安全性.

(3) 从水印嵌入域的选择来看, 绝大多数算法在实现版权保护的鲁棒水印模块选择 DWT 及其变体 LWT, SWT 等作用后的频域, 是因为水印嵌入小波分解后的低频区域可保证基本的鲁棒性. 为进一步提高水印抵抗几何攻击的能力, 同时结合 SVD, LU 等矩阵分解的混合域成为鲁棒水印模块的首选. 在实现篡改检测与定位的水印模块, 大多算法选择空域、频域的高频成分嵌入水印, 可对篡改敏感.

(4) 从水印提取的方式来看, 考虑到非盲提取时所需原载体、水印信息的存储成本与安全性, 设计盲提取水印算法更加通用和流行. 而水印提取方式与嵌入方法息息相关, 多数基于 LSB、基于关系、基于量化嵌入的算法都实现了盲提取. 线性融合方法虽然简单、能够嵌入大容量信息, 曾在一段时期内备受青睐, 但不能实现盲提取, 逐渐被研究人员弃用.

(5) 从算法嵌入的水印类型来看, 目前在多功能图像水印算法中, 篡改检测与定位水印多为给定或自生成的二值信息, 版权、鲁棒水印多为二值图像, 少数为灰度图像, 罕有算法选择把彩色图像作为鲁棒水印. 原因是嵌入大量水印信息不可保证载体图像的质量.

(6) 从水印优化角度来看, 越来越多的算法选择在方法中结合 ABC 和 PSO 等启发式算法, 以平衡水印的鲁棒性与不可见性; 结合 SIFT 和 SURF 等特征提取方法, 提高鲁棒水印抗几何攻击能力; 结合 LZW 等压缩方法提高水印嵌入容量.

4　相关研究趋势

通过对当前数字图像多功能水印算法的分析, 本节对该领域存在的问题给出可能的解决方案, 尝试展望数字图像多功能水印技术未来的发展趋势.

(1) 设计嵌入彩色鲁棒水印的图像多功能水印算法. 目前, 多功能水印算法中的鲁棒水印尚未使用彩色图像, 一方面是因为相同尺寸的彩色水印需要嵌入的位数的是灰度水印的 3 倍, 二值水印的 24 倍. 多功能水印算法已嵌入多种水印, 再增加过多的嵌入量会对载体质量产生更大影响. 另一方面是因为在嵌入方法与载体图像尺寸的限制下, 实现彩色水印的盲提取难度大. 但目前大量版权图像为彩色图像, 因此, 实现彩色鲁棒水印嵌入的多功能水印势在必行. 可尝试从 3 个方面进行改善. 首先, 在嵌入水印前使用压缩方法减少水印实际嵌入量; 其次, 可以通过扩大水印嵌入域的方式嵌入更多水印, 如 RDWT 与 DWT 相比, 变换后的逼近、细节子带大小都与原图像相同, 故能嵌入更多的水印信息; 除此之外, 为十进制数据设计盲提取算法也是值得关注的问题.

(2) 设计能应用在真实场景的图像多功能水印算法. 目前, 在实验室环境下, 多功能图像水印算法常使用脆弱水印完成篡改检测与定位, 但图像在网络传输中受到 JPEG 压缩是不可避免的情况, 这并非篡改了图像内容, 但仍会使脆弱水印生效, 最终影响对内容篡改的判断. 因此, 在实际应用场景中实现图像篡改检测与定位的水印必然要有能力抵抗 JPEG 等一系列常见压缩, 同时对内容篡改敏感. 因此, 半脆弱水印比脆弱水印更适合与鲁棒水印结合去实现多功能.

(3) 设计与新技术结合的图像多功能水印算法. 目前, 深度学习与人工智能在图像处理领域的优势使得单水印算法设计了与深度学习模型结合的方案. 但在多功能水印领域, 应用此类技术的算法甚少, 未来的工作可以考虑结合这些新技术去提升算法的性能.

(4) 设计具有良好性能的图像多功能水印算法. 尽管目前很多水印算法实现了双功能, 有些甚至实现了三功能, 但鲜有算法可以同时在版权保护、篡改检测与定位、篡改区域恢复方面都取得良好性能. 从多水印嵌入后的不可见性、鲁棒性、篡改检测的精度、篡改恢复的效果来看, 数字图像多功能水印算法存在较大的提升空间.

5　结　语

数字图像水印技术作为信息隐藏的重要分支, 是信息安全领域长期的研究热点之一. 其核心在于在不影响载体图像使用价值的前提下, 通过嵌入与图像相关的信息, 实现版权保护、所有权认证、完整性认证、篡改恢复等保护功能. 尽管传统的数字图像单水印技术已经得到深入发展与广泛应用, 但多功能水印因其自身特性, 不能完全照搬

单水印技术的工作成果. 因此, 同时实现多种保护功能的数字图像多功能水印技术仍有很大的发展空间.

本文从基础概念、常用技术、应用场景等方面对数字图像水印技术的基本原理与研究现状进行了归纳; 以多水印嵌入方式为分类标准对近 10 年的图像多功能水印算法进行了梳理与综述; 以各模型与算法的优缺点对比为牵引, 总结了当前多功能水印技术的发展现状并对未来发展方向做出展望. 分析结果表明, 在实现多功能时, 多水印嵌入载体图像难免会对水印的综合性能造成损失, 且图像多功能水印算法在真实应用场景中的效果有待提升. 期望研究者未来能够将人工智能, 特别是计算机视觉领域的知识应用于图像多功能水印, 以有效提高水印嵌入容量、不可见性及鲁棒性, 提升篡改定位的精确性.

参考文献(References):

[1] Wan W B, Wang J, Zhang Y M, *et al*. A comprehensive survey on robust image watermarking[J]. Neurocomputing, 2022, 488: 226-247

[2] Zhang Yi, Luo Xiangyang, Wang Jinwei, *et al*. Research progress on digital image robust steganography[J]. Journal of Image and Graphics, 2022, 27(1): 3-26(in Chinese)
(张祎, 罗向阳, 王金伟, 等. 数字图像鲁棒隐写综述[J]. 中国图象图形学报, 2022, 27(1): 3-26)

[3] Barnett R. Digital watermarking: applications, techniques and challenges[J]. Electronics & Communication Engineering Journal, 1999, 11(4): 173-183

[4] Begum M, Ferdush J, Uddin M S. A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(8): 5856-5867

[5] Moosazadeh M, Ekbatanifard G. A new DCT-based robust image watermarking method using teaching-learning-based optimization[J]. Journal of Information Security and Applications, 2019, 47: 28-38

[6] Liu Y, Tang S Y, Liu R, *et al*. Secure and robust digital image watermarking scheme using logistic and RSA encryption[J]. Expert Systems with Applications, 2018, 97: 95-105

[7] Molina-Garcia J, Garcia-Salgado B P, Ponomaryov V, *et al*. An effective fragile watermarking scheme for color image tampering detection and self-recovery[J]. Signal Processing: Image Communication, 2020, 81: Article No.115725

[8] Qin C, Ji P, Zhang X P, *et al*. Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy[J]. Signal Processing, 2017, 138: 280-293

[9] Haghighi B B, Taherinia A H, Harati A. TRLH: fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique[J]. Journal of Visual Communication and Image Representation, 2018, 50: 49-64

[10] Huo Y R, Liu J J, Zhang Q, *et al*. Semi-fragile watermarking for color image authentication in power internet of things[C] // Proceedings of the IEEE Innovative Smart Grid Technologies-Asia. Los Alamitos: IEEE Computer Society Press, 2019: 2865-2869

[11] Ouyang J L, Huang J T, Wen X Z, *et al*. A semi-fragile watermarking tamper localization method based on QDFT and multi-view fusion[J]. Multimedia Tools and Applications, 2023, 82(10): 15113-15141

[12] Sikder I, Dhar P K, Shimamura T. Semi-fragile watermarking method using slant transform and LU decomposition for image authentication[C] //Proceedings of the International Conference on Electrical, Computer and Communication Engineering. Los Alamitos: IEEE Computer Society Press, 2017: 881-885

[13] Aminuddin A, Ernawan F. AuSR1: authentication and self- recovery using a new image inpainting technique with LSB shifting in fragile image watermarking[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(8): 5822-5840

[14] Huang L, Kuang D, Li C L, *et al*. A self-embedding secure fragile watermarking scheme with high quality recovery[J]. Journal of Visual Communication and Image Representation, 2022, 83: Article No.103437

[15] Lu Z M, Xu D G, Sun S H. Multipurpose image watermarking algorithm based on multistage vector quantization[J]. IEEE Transactions on Image Processing, 2005, 14(6): 822-831

[16] Yuan J, Cui G H, Zhang Y J. A practical multipurpose color image watermarking algorithm for copyright protection and image authentication[C] //Proceedings of the International Conference on Digital Telecommunications. Los Alamitos: IEEE Computer Society Press, 2006: 72-72

[17] Lu C S, Liao H Y M. Multipurpose watermarking for image authentication and protection[J]. IEEE Transactions on Image Processing, 2001, 10(10): 1579-1592

[18] Thabit R. Review of medical image authentication techniques and their recent trends[J]. Multimedia Tools and Applications, 2021, 80(9): 13439-13473

[19] Evsutin O, Dzhanashia K. Watermarking schemes for digital images: robustness overview[J]. Signal Processing: Image Communication, 2022, 100: Article No.116523

[20] Begum M, Uddin M S. Digital image watermarking techniques: a review[J]. Information, 2020, 11(2): Article No.110

[21] Yu X Y, Wang C Y, Zhou X. Review on semi-fragile watermarking algorithms for content authentication of digital images[J]. Future Internet, 2017, 9(4): Article No.56

[22] Li Zhaohong, Hou Jianjun. DCT-domain fragile watermarking algorithm based on Logistic maps[J]. Acta Electronica Sinica, 2006, 34(12): 2134-2137(in Chinese)
(李赵红. 侯建军. 基于 Logistic 混沌映射的 DCT 域脆弱数字水印算法[J]. 电子学报, 2006, 34(12): 2134-2137)

[23] Tang Guoping, Liao Xiaofeng. A resisting cropping robust watermarking algorithm based on chaotic map[J]. Computer Engineering, 2005, 31(9): 34-36(in Chinese)
(唐国坪, 廖晓峰. 基于混沌映射的抗剪切鲁棒水印算法[J]. 计算机工程, 2005, 31(9): 34-36)

[24] Liu Fang, Jia Cheng, Yuan Zheng. Watermarking in binary image based on Arnold transformation[J]. Journal of Computer Applications, 2008, 28(6): 1404-1406, 1410(in Chinese)
(刘芳, 贾成, 袁征. 一种基于 Arnold 变换的二值图像水印算法[J]. 计算机应用, 2008, 28(6): 1404-1406, 1410)

[25] Feng Maoyan, Feng Bo, Shen Chunlin. Adaptive image watermarking algorithm based on block DCT transform and Arnold shuffling[J]. Journal of Computer Applications, 2008, 28(1): 171-173(in Chinese)
(冯茂岩, 冯波, 沈春林. 基于分块 DCT 变换和 Arnold 置乱的自适应图像水印算法[J]. 计算机应用, 2008, 28(1): 171-173)

[26] Ou Bo, Li Xiaolong, Ni Rongrong, *et al*. Review of reversible data hiding in images[J]. Journal of Beijing Jiaotong University, 2022, 46(1): 1-10(in Chinese)
(欧博, 李晓龙, 倪蓉蓉, 等. 图像可逆信息隐藏研究发展综述[J]. 北京交通大学学报, 2022, 46(1): 1-10)

[27] Liu J, He X J. A review study on digital watermarking[C] // Proceedings of the International Conference on Information and Communication Technologies. Los Alamitos: IEEE Computer Society Press, 2005: 337-341

[28] Wan W B, Wang J, Li J, *et al*. Hybrid JND model-guided watermarking method for screen content images[J]. Multimedia Tools and Applications, 2020, 79(7-8): 4907-4930

[29] Al-Otum H M. Secure and robust host-adapted color image watermarking using inter-layered wavelet-packets[J]. Journal of Visual Communication and Image Representation, 2020, 66: Article No.102726

[30] Alshoura W H, Zainol Z, Teh J S, *et al*. Hybrid SVD-based image watermarking schemes: a review[J]. IEEE Access, 2021, 9: 32931-32968

[31] van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark[C] //Proceedings of the 1st International Conference on Image Processing. Los Alamitos: IEEE Computer Society Press, 1994: 86-90

[32] Zhang W Y, Shih F Y. Semi-fragile spatial watermarking based on local binary pattern operators[J]. Optics Communications, 2011, 284(16-17): 3904-3912

[33] Badran E F, Sharkas M A, Attallah O A. Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images[C] //Proceedings of the National Radio Science Conference. Los Alamitos: IEEE Computer Society Press, 2009: 1-8

[34] Zeki A M, Manaf A A. A novel digital watermarking technique based on ISB (Intermediate Significant Bit)[J]. World Academy of Science, Engineering and Technology, 2009, 50: 989-996

[35] Mohammed G N, Yasin A, Zeki A M. Robust image watermarking based on dual intermediate significant bit (DISB)[C] // Proceedings of the 6th International Conference on Computer Science and Information Technology. Los Alamitos: IEEE Computer Society Press, 2014: 18-22

[36] Kuang X, Ling W A, Ke L S, *et al*. Watermark embedding and extraction based on LSB and four-step phase shift method[C] // Proceedings of the 7th International Conference on Information Technology: IoT and Smart City. New York: ACM Press, 2019: 243-247

[37] Huynh-The T, Lee S. Color image watermarking using selective MSB-LSB embedding and 2D otsu thresholding[C] // Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. Los Alamitos: IEEE Computer Society Press, 2017: 1333-1338

[38] Muyco S D, Hernandez A A. Least significant bit hash algorithm for digital image watermarking authentication[C] // Proceedings of the 5th International Conference on Computing and Artificial Intelligence. New York: ACM Press, 2019: 150-154

[39] Bender W, Gruhl D, Morimoto N, *et al*. Techniques for data hiding[J]. IBM Systems Journal, 1996, 35(3-4): 313-336

[40] Chen W T, Zhu C Q, Ren N, *et al*. Screen-cam robust and blind watermarking for tile satellite images[J]. IEEE Access, 2020, 8: 125274-125294

[41] Kang J, Hou J U, Ji S, *et al*. Robust spherical panorama image watermarking against viewpoint desynchronization[J]. IEEE Access, 2020, 8: 127477-127490

[42] Hsu L Y, Hu H T. Robust blind image watermarking using crisscross inter-block prediction in the DCT domain[J]. Journal of Visual Communication and Image Representation, 2017, 46: 33-47

[43] Cox I J, Kilian J, Leighton F T, *et al*. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687

[44] Sisaudia V, Vishwakarma V P. Copyright protection using KELM-PSO based multi-spectral image watermarking in DCT domain with local texture information based selection[J]. Multimedia Tools and Applications, 2021, 80(6): 8667-8688

[45] Koch E, Zhao J. Towards robust and hidden image copyright labeling[C] //Proceedings of the IEEE Workshop on Nonlinear Signal and Image Processing. Los Alamitos: IEEE Computer Society Press, 1995: 123-132

[46] Gupta M, Rama Kishore R. Secured blind image watermarking using entropy technique in DCT domain[M] //Gupta D, Khanna A, Kansal V, *et al*. Proceedings of Second Doctoral Symposium on Computational Intelligence. Heidelberg: Springer, 2022: 31-47

[47] Abraham J, Paul V. An imperceptible spatial domain color image watermarking scheme[J]. Journal of King Saud University-Computer and Information Sciences, 2019, 31(1): 125-133

[48] Hsu C T, Wu J L. Multiresolution watermarking for digital images[J]. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 1998, 45(8): 1097-1101

[49] Giri K J, Quadri S M K, Bashir R, *et al*. DWT based color image watermarking: a review[J]. Multimedia Tools and Applications, 2020, 79(43-44): 32881-32895

[50] Lee Y S, Seo Y H, Kim D W. Blind image watermarking based on adaptive data spreading in n-level DWT subbands[J]. Security and Communication Networks, 2019, 2019: Article No.8357251

[51] Gao Y C, Wang J W, Shi Y Q. Dynamic multi-watermarking and detecting in DWT domain[J]. Journal of Real-Time Image Processing, 2019, 16(3): 565-576

[52] Awasthi D, Srivastava V K. Robust, imperceptible and optimized watermarking of DICOM image using Schur decomposition, LWT-DCT-SVD and its authentication using SURF[J]. Multimedia Tools and Applications, 2023, 82(11): 16555-16589

[53] Singh O P, Singh A K. Image fusion-based watermarking in IWT-SVD domain[M] //Gupta D, Sambyo K, Prasad M, *et al*. Advanced Machine Intelligence and Signal Processing. Heidelberg: Springer, 2022: 163-175

[54] Li M J, Yuan X C. Adaptive segmentation-based feature extraction and S-STDM watermarking method for color image[J]. Neural Computing and Applications, 2020, 32(13): 9181-9200

[55] Khare P, Srivastava V K. A secured and robust medical image watermarking approach for protecting integrity of medical images[J]. Transactions on Emerging Telecommunications Technologies, 2021, 32(2): Article No.e3918

[56] Liu J, Li J B, Ma J X, *et al*. A robust multi-watermarking algorithm for medical images based on DTCWT-DCT and Henon map[J]. Applied Sciences, 2019, 9(4): Article No.700

[57] Liu R Z, Tan T N. An SVD-based watermarking scheme for protecting rightful ownership[J]. IEEE Transactions on Multimedia, 2002, 4(1): 121-128

[58] Cai Yijia, Niu Yugang, Su Qingtang. Blind watermarking algorithm for color images based on DWT-SVD and Fibonacci transformation[J]. Application Research of Computers, 2012, 29(8): 3025-3028(in Chinese)
(蔡宜嘉, 牛玉刚, 苏庆堂. 基于DWT-SVD和Fibonacci变换的彩色图像盲水印算法[J]. 计算机应用研究, 2012, 29(8): 3025-3028)

[59] Su Q T, Wang G, Zhang X F, *et al*. A new algorithm of blind color image watermarking based on LU decomposition[J]. Multidimensional Systems and Signal Processing, 2018, 29(3): 1055-1074

[60] Li J Z, Yu C Y, Gupta B B, *et al*. Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition[J]. Multimedia Tools and Applications, 2018, 77(4): 4545-4561

[61] Nha P T, Thanh T M, Phong N T. Consideration of a robust watermarking algorithm for color image using improved *QR* decomposition[J]. Soft Computing, 2022, 26(11): 5069-5093

[62] Su Q T, Chen B J. A novel blind color image watermarking using upper Hessenberg matrix[J]. AEU-International Journal of Electronics and Communications, 2017, 78: 64-71

[63] Su Qingtang. Digital blind watermarking technology for color images[M]. Beijing: Tsinghua University Press, 2015(in Chinese)
(苏庆堂. 彩色图像数字盲水印技术[M]. 北京: 清华大学出版社, 2015)

[64] Do M N, Vetterli M. The contourlet transform: an efficient directional multiresolution image representation[J]. IEEE Transactions on Image Processing, 2005, 14(12): 2091-2106

[65] Thomas R, Sucharitha M. Contourlet and gould transforms for hybrid image watermarking in RGB color images[J]. Intelligent Automation & Soft Computing, 2022, 33(2): 879-889

[66] Zhang Y F, Sun Y B. An image watermarking method based on visual saliency and contourlet transform[J]. Optik, 2019, 186: 379-389

[67] Koley S. Bat optimized 3D anaglyph image watermarking based on maximum noise fraction in the digital shearlet domain[J]. Multimedia Tools and Applications, 2022, 81(14): 19491-19523

[68] Hadad A A A, Khalid H N, Naser Z S, *et al*. A robust color image watermarking scheme based on discrete wavelet transform domain and discrete slantlet transform technique[J]. Ingénierie des Systèmes d Information, 2022, 27(2): 313-319

[69] Mundher M, Muhamad D, Rehman A, *et al*. Digital watermarking for images security using discrete slantlet transform[J]. Applied Mathematics & Information Sciences, 2014, 8(6): 2823-2830

[70] Koolwal P, Sharma S. Performance improvement of optimization algorithm for digital image watermarking in hybrid DWT-DCT transform[C] //Proceedings of the International Conference on Electronics and Renewable Systems. Los Alamitos: IEEE Computer Society Press, 2022: 1001-1005

[71] Deb K, Al-Seraj S, Hoque M, *et al*. Combined DWT-DCT based digital image watermarking technique for copyright protection[C] //Proceedings of the 7th International Conference on Electrical and Computer Engineering. Los Alamitos: IEEE Computer Society Press, 2012: 458-461

[72] Anand A, Singh A K. An improved DWT-SVD domain watermarking for medical information security[J]. Computer Communications, 2020, 152: 72-80

[73] Ganic E, Eskicioglu A M. Robust DWT-SVD domain image watermarking: embedding data in all frequencies[C] //Proceedings of the Workshop on Multimedia and Security. New York: ACM Press, 2004: 166-174

[74] Sun X X, Pan J S, Weng S W, *et al*. Optimization of MSFs for watermarking using DWT-DCT-SVD and fish migration optimization with QUATRE[J]. Multimedia Tools and Applications, 2023, 82(2): 2255-2276

[75] Zear A, Singh A K, Kumar P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine[J]. Multimedia Tools and Applications, 2018, 77(4): 4863-4882

[76] Cox I J, Kilian J, Leighton T, *et al*. A secure, robust watermark for multimedia[C] //Proceedings of the 1st International Workshop on Information Hiding. Heidelberg: Springer, 1996: 185-206

[77] Chen B, Wornell G W. Quantization index modulation methods for digital watermarking and information embedding of multimedia[J]. Journal of VLSI Signal Processing Systems for Signal, Image and Video Technology, 2001, 27(1-2): 7-33

[78] Chen B, Wornell G W. Digital watermarking and information embedding using dither modulation[C] //Proceedings of the IEEE 2nd Workshop on Multimedia Signal Processing. Los Alamitos: IEEE Computer Society Press, 1998: 273-278

[79] Li Q, Doerr G, Cox I J. Spread transform dither modulation using a perceptual model[C] //Proceedings of the IEEE Workshop on Multimedia Signal Processing. Los Alamitos: IEEE Computer Society Press, 2006: 98-102

[80] Hatoum M W, Darazi R, Couchot J F. Normalized blind STDM watermarking scheme for images and PDF documents robust against fixed gain attack[J]. Multimedia Tools and Applications, 2020, 79(3-4): 1887-1919

[81] Pérez-González F, Mosquera C, Barni M, *et al*. Rational dither modulation: a high-rate data-hiding method invariant to gain attacks[J]. IEEE Transactions on Signal Processing, 2005, 53(10): 3960-3975

[82] Kalantari N K, Ahadi S M. A logarithmic quantization index

modulation for perceptually better data hiding[J]. IEEE Transactions on Image Processing, 2010, 19(6): 1504-1517

[83] Wang J, Wan W B, Li X X, *et al*. Color image watermarking based on orientation diversity and color complexity[J]. Expert Systems with Applications, 2020, 140: Article No.112868

[84] Huang Y, Niu B N, Guan H, *et al*. Enhancing image watermarking with adaptive embedding parameter and PSNR guarantee[J]. IEEE Transactions on Multimedia, 2019, 21(10): 2447-2460

[85] Huang Ying, Niu Baoning, Guan Hu, *et al*. Image texture based adaptive watermarking algorithm[J]. Journal of Beijing University of Aeronautics and Astronautics, 2019, 45(12): 2403-2414(in Chinese)
(黄樱, 牛保宁, 关虎, 等. 基于图像纹理的自适应水印算法[J]. 北京航空航天大学学报, 2019, 45(12): 2403-2414)

[86] Swaraja K, Meenakshi K, Kora P. An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine[J]. Biomedical Signal Processing and Control, 2020, 55: Article No.101665

[87] Koley S. Visual attention model based dual watermarking for simultaneous image copyright protection and authentication[J]. Multimedia Tools and Applications, 2021, 80(5): 6755-6783

[88] Sinhal R, Ansari I A. Multipurpose image watermarking: ownership check, tamper detection and self-recovery[J]. Circuits, Systems, and Signal Processing, 2022, 41(6): 3199-3221

[89] Wen Quan, Sun Tanfeng, Wang Shuxun. Concept and application of zero-watermark[J]. Acta Electronica Sinica, 2003, 31(2): 214-216(in Chinese)
(温泉, 孙锬锋, 王树勋. 零水印的概念与应用[J]. 电子学报, 2003, 31(2): 214-216)

[90] Xiang Hua, Cao Hanqiang, Wu Kaining, *et al*. A zero- watermarking algorithm based on chaotic modulation[J]. Journal of Image and Graphics, 2006, 11(5): 720-724(in Chinese)
(向华, 曹汉强, 伍凯宁, 等. 一种基于混沌调制的零水印算法[J]. 中国图象图形学报, 2006, 11(5): 720-724)

[91] Wang Yifei, Zhou Yangming, Qian Zhenxing, *et al*. Review of robust video watermarking[J]. Journal of Image and Graphics, 2022, 27(1): 27-42(in Chinese)
(王翌妃, 周杨铭, 钱振兴, 等. 鲁棒视频水印研究进展[J]. 中国图象图形学报, 2022, 27(1): 27-42)

[92] Kandi H, Mishra D, Gorthi S R K S. Exploring the learning capabilities of convolutional neural networks for robust image watermarking[J]. Computers & Security, 2017, 65: 247-268

[93] Mun S M, Nam S H, Jang H U, *et al*. A robust blind watermarking using convolutional neural network[OL]. [2022-11-21]. https://arxiv.org/abs/1704.03248

[94] Krizhevsky A, Sutskever I, Hinton G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90

[95] Hayes J, Danezis G. Generating steganographic images via adversarial training[C] //Proceedings of the 31st International Conference on Neural Information Processing Systems. New York: ACM Press, 2017: 1951-1960

[96] Zhang K A, Cuesta-Infante A, Xu L, *et al*. SteganoGAN: high capacity image steganography with GANs[OL]. [2022-11-21]. https://arxiv.org/abs/1901.03892

[97] Zhu J R, Kaplan R, Johnson J, *et al*. HiDDeN: hiding data with deep networks[C] //Proceedings of the 15th European Conference on Computer Vision. Heidelberg: Springer, 2018: 657-672

[98] Ahmadi M, Norouzi A, Karimi N, *et al*. ReDMark: framework for residual diffusion watermarking based on deep networks[J]. Expert Systems with Applications, 2020, 146: Article No.113157

[99] Jia Z Y, Fang H, Zhang W M. MBRS: enhancing robustness of DNN-based watermarking by mini-batch of real and simulated JPEG compression[C] //Proceedings of the 29th ACM International Conference on Multimedia. New York: ACM Press, 2021: 41-49

[100] Liu K L, Chen D D, Liao J, *et al*. JPEG robust invertible grayscale[J]. IEEE Transactions on Visualization and Computer Graphics, 2022, 28(12): 4403-4417

[101] Hamamoto I, Kawamura M. Neural watermarking method including an attack simulator against rotation and compression attacks[J]. IEICE Transactions on Information and Systems, 2020, E103.D(1): 33-41

[102] Luo X Y, Zhan R H, Chang H W, *et al*. Distortion agnostic deep watermarking[C] //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Los Alamitos: IEEE Computer Society Press, 2020: 13548-13557

[103] Tancik M, Mildenhall B, Ng R. StegaStamp: invisible hyperlinks in physical photographs[C] //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Los Alamitos: IEEE Computer Society Press, 2020: 2117-2126

[104] Ge S L, Fei J W, Xia Z H, *et al*. A screen-shooting resilient document image watermarking scheme using deep neural network[J]. IET Image Processing, 2023, 17(2): 323-336

[105] Zhang R, Isola P, Efros A A, *et al*. The unreasonable effectiveness of deep features as a perceptual metric[C] //Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Los Alamitos: IEEE Computer Society Press, 2018: 586-595

[106] Liu Y, Guo M X, Zhang J, *et al*. A novel two-stage separable deep learning framework for practical blind watermarking[C] //Proceedings of the 27th ACM International Conference on Multimedia. New York: ACM Press, 2019: 1509-1517

[107] Zhang C N, Karjauv A, Benz P, *et al*. Towards robust deep hiding under non-differentiable distortions for practical blind watermarking[C] //Proceedings of the 29th ACM International Conference on Multimedia. New York: ACM Press, 2021: 5158-5166

[108] Yu C. Attention based data hiding with generative adversarial networks[C] //Proceedings of the 34th AAAI Conference on Artificial Intelligence. Palo Alto: AAAI Press, 2020: 1120-1128

[109] Hao K L, Feng G R, Zhang X P. Robust image watermarking based on generative adversarial network[J]. China Communications, 2020, 17(11): 131-140

[110] Li L D, Li S S, Abraham A, *et al*. Geometrically invariant image watermarking using polar harmonic transforms[J]. Information Sciences, 2012, 199: 1-19

[111] Hu R W, Xiang S J. Lossless robust image watermarking by

using polar harmonic transform[J]. Signal Processing, 2021, 179: Article No.107833

[112] Zhu D D, Zhang X P, Zhang Y L, *et al*. A new image watermarking algorithm using NSCT and Harris detector in green manufacturing[J]. Applied Mechanics and Materials, 2013, 340: 277-282

[113] Liu Ying, Yang Xing, Zhu Tingge. Robust watermarking algorithm based on structured forests edge and SIFT[J]. Laser & Optoelectronics Progress, 2021, 58(6): Article No.0615006 (in Chinese)
(刘颖, 杨星, 朱婷鸽. 基于结构森林边缘和 SIFT 的鲁棒水印算法[J]. 激光与光电子学进展, 2021, 58(6): Article No.0615006)

[114] Hou Xiang, Min Lianquan. A robust watermarking algorithm using SURF feature regions[J]. Geomatics and Information Science of Wuhan University, 2017, 42(3): 412-426(in Chinese)
(侯翔, 闵连权. 基于 SURF 特征区域的鲁棒水印算法[J]. 武汉大学学报(信息科学版), 2017, 42(3): 421-426)

[115] Pourhadi A, Mahdavi-Nasab H. A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain[J]. Multimedia Tools and Applications, 2020, 79(29-30): 21653-21677

[116] Li Yingying, Zhang Yifeng, Cheng Xu, *et al*. Robust watermarking algorithm based on DWT optimal multi-subgraph and SIFT geometric correction[J]. Application Research of Computers, 2019, 36(6): 1819-1823, 1827(in Chinese)
(李莹莹, 张毅锋, 程旭, 等. 基于DWT最优多子图和SIFT几何校正的鲁棒水印算法[J]. 计算机应用研究, 2019, 36(6): 1819-1823, 1827)

[117] Sivananthamaitrey P, Kumar P R. Optimal dual watermarking of color images with SWT and SVD through genetic algorithm[J]. Circuits, Systems, and Signal Processing, 2022, 41(1): 224-248

[118] Ansari I A, Pant M. Multipurpose image watermarking in the domain of DWT based on SVD and ABC[J]. Pattern Recognition Letters, 2017, 94: 228-236

[119] Laxmanika, Singh P K. Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain[J]. Multimedia Tools and Applications, 2022, 81(16): 22001-22026

[120] Salimi L, Haghighi A, Fathi A. A novel watermarking method based on differential evolutionary algorithm and wavelet transform[J]. Multimedia Tools and Applications, 2020, 79(17-18): 11357-11374

[121] Hassan O M S, Abdulazeez A M, Mohammed A I, *et al*. An efficient robust color watermarking algorithm based on DWT, DCT, BFO and implementation[C] //Proceedings of the IEEE 11th International Conference on System Engineering and Technology. Los Alamitos: IEEE Computer Society Press, 2021: 90-95

[122] Haghighi B B, Taherinia A H, Harati A, *et al*. WSMN: an optimized multipurpose blind watermarking in Shearlet domain using MLP and NSGA-II[J]. Applied Soft Computing, 2021, 101: Article No.107029

[123] Lefèvre P, Carré P, Fontaine C, *et al*. Efficient image tampering localization using semi-fragile watermarking and error control codes[J]. Signal Processing, 2022, 190: Article No.108342

[124] Wang Yilong, Li Zhenyu, Gong Daofu, *et al*. Image self- embedding semi-fragile watermarking algorithm based on block truncation coding[J]. Journal of Image and Graphics, 2022, 27(1): 203-214(in Chinese)
(王艺龙, 李震宇, 巩道福, 等. 块截断编码的图像自嵌入半脆弱水印算法[J]. 中国图象图形学报, 2022, 27(1): 203-214)

[125] Zhang M M, Ni R R, Zhao Y. A blind print-recapture robust watermark scheme by calculating self-convolution[J]. International Journal of Digital Crime and Forensics, 2019, 11(4): 28-49

[126] Li F Q, Wang S L. Persistent watermark for image classification neural networks by penetrating the autoencoder[C] // Proceedings of the IEEE International Conference on Image Processing. Los Alamitos: IEEE Computer Society Press, 2021: 3063-3067

[127] Li Xiaolong, Yu Nenghai, Zhang Xinpeng, *et al*. Overview of digital media forensics technology[J]. Journal of Image and Graphics, 2021, 26(6): 1216-1226(in Chinese)
(李晓龙, 俞能海, 张新鹏, 等. 数字媒体取证技术综述[J]. 中国图象图形学报, 2021, 26(6): 1216-1226)

[128] Rao Y, Ni J Q, Zhang W Z, *et al*. Towards JPEG-resistant image forgery detection and localization via self-supervised domain adaptation[J/OL]. IEEE Transactions on Pattern Analysis and Machine Intelligence: 1-12 [2022-11-21]. https://ieeexplore.ieee.org/abstract/document/9904872

[129] Niu Yakun, Zhao Yao, Li Xiaolong. Research progress of JPEG image passive forensics[J]. Journal of Signal Processing, 2022, 38(6): 1170-1179(in Chinese)
(牛亚坤, 赵耀, 李晓龙. JPEG 图像被动取证研究进展综述[J]. 信号处理, 2022, 38(6): 1170-1179)

[130] Zhou Linna, Yang Zhen, Chu Beilin, *et al*. Overview of multimedia cognition security[J]. Journal of Signal Processing, 2021, 37(12): 2440-2456(in Chinese)
(周琳娜, 杨震, 储贝林, 等. 多媒体认知安全综述[J]. 信号处理, 2021, 37(12): 2440-2456)

[131] Wang Renying, Chu Beilin, Yang Zhen, *et al*. An overview of visual DeepFake detection techniques[J]. Journal of Image and Graphics, 2022, 27(1): 43-62(in Chinese)
(王任颖, 储贝林, 杨震, 等. 视觉深度伪造检测技术综述[J]. 中国图象图形学报, 2022, 27(1): 43-62)

[132] Fares K, Khaldi A, Redouane K, *et al*. DCT & DWT based watermarking scheme for medical information security[J]. Biomedical Signal Processing and Control, 2021, 66: Article No.102403

[133] Paikaray B K, Swain D, Chakravarty S. An improved region-based embedding technique for data hiding and image recovery using multiple ROI and RONI[J]. International Journal of Electronic Security and Digital Forensics, 2023, 15(2): 101-113

[134] Sharkas M, ElShafie D, Hamdy N. A dual digital-image watermarking technique[J]. International Journal of Computer and Information Engineering, 2007, 1(5): 1477-1480

[135] 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

[136] Li Y W, Song W, Zhao X B, *et al*. A novel image tamper detec-

tion and self-recovery algorithm based on watermarking and chaotic system[J]. Mathematics, 2019, 7(10): Article No.955

[137] Wang C Y, Zhang H, Zhou X. A self-recovery fragile image watermarking with variable watermark capacity[J]. Applied Sciences, 2018, 8(4): Article No.548

[138] Chen Fan, He Hongjie, Wang Hongxia. Variable-payload self-recovery watermarking scheme for digital image authentication[J]. Chinese Journal of Computers, 2012, 35(1): 154-162(in Chinese)
(陈帆，和红杰，王宏霞. 用于图像认证的变容量恢复水印算法[J]. 计算机学报, 2012, 35(1): 154-162)

[139] Tarhouni N, Charfeddine M, Ben Amar C. Novel and robust image watermarking for copyright protection and integrity control[J]. Circuits, Systems, and Signal Processing, 2020, 39(10): 5059-5103

[140] Ye Tianyu. A self-embedding image watermarking scheme with dual purpose[J]. Acta Photonica Sinica, 2012, 41(7): 859-867(in Chinese)
(叶天语. 自嵌入双功能图像水印算法[J]. 光子学报, 2012, 41(7): 859-867)

[141] Ye Tianyu. Perfectly blind image watermarking scheme with multi-purpose based on region segment for sub-block and self-embedding technology[J]. Journal on Communications, 2013, 34(3): 148-156(in Chinese)
(叶天语. 基于子块区域分割和自嵌入技术的全盲多功能图像水印算法[J]. 通信学报, 2013, 34(3): 148-156)

[142] Zhu Guang, Shi Wen, Zhu Xuefang, *et al*. Multi-purpose watermark algorithm of color images based on SURF[J]. Journal of Image and Graphics, 2013, 18(12): 1694-1702(in Chinese)
(朱光，师文，朱学芳，等. 结合 SURF 特征的多功能彩色图像水印算法[J]. 中国图象图形学报，2013，18(12)：1694-1702)

[143] Zhao Chunhui, Liu Wei. Mutual support dual watermark algorithm based on compressive sensing[J]. Acta Electronica Sinica, 2012, 40(4): 681-687(in Chinese)
(赵春晖，刘巍. 基于压缩感知的交互支持双水印算法[J]. 电子学报, 2012, 40(4): 681-687)

[144] Zhao Yanxia, Wang Xizhao. Multipurpose zero watermarking algorithm for color image based on SVD and DCNN[J]. Journal of Shandong University (Engineering Science), 2018, 48(3): 25-33(in Chinese)
(赵彦霞，王熙照. 基于 SVD 和 DCNN 的彩色图像多功能零水印算法[J]. 山东大学学报(工学版), 2018, 48(3): 25-33)

[145] Meng Z X, Morizumi T, Miyata S, *et al*. Design scheme of copyright management system based on digital watermarking and blockchain[C] //Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference. Los Alamitos: IEEE Computer Society Press, 2018: 359-364

[146] Wang B W, Shi J W, Wang W S, *et al*. Image copyright protection based on blockchain and zero-watermark[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(4): 2188-2199

[147] Lv Jianping, Liu Qi. Bifunctional watermarking algorithm based on chaos theory and quantitative methods[J]. Journal of Xi'an University of Posts and Telecommunications, 2014, 19(3): 54-57, 83(in Chinese)
(吕建平，刘齐. 基于混沌理论和量化方法的双功能水印算法[J]. 西安邮电大学学报, 2014, 19(3): 54-57+83)

[148] Kunhu A, Al-Ahmad H. A new multi watermarking algorithm based on DWT and hash functions for color satellite images[C] //Proceedings of the IEEE 20th International Conference on Electronics, Circuits, and Systems. Los Alamitos: IEEE Computer Society Press, 2013: 429-432

[149] Ansari I A, Pant M, Ahn C W, *et al*. PSO optimized multipurpose image watermarking using SVD and chaotic sequence[C] // Proceedings of the 10th Bio-Inspired Computing - Theories and Applications. Heidelberg: Springer, 2015: 1-17

[150] Chen Shanxue, Qi Ruolan, Tang Yiyuan. Multi-purpose watermark algorithm for color image based on multiple transform domains[J]. Journal of Computer Applications, 2018, 38(8): 2274-2279, 2286(in Chinese)
(陈善学，漆若兰，唐义嫄. 基于多变换域的彩色图像多功能水印算法[J]. 计算机应用, 2018, 38(8): 2274-2279, 2286)

[151] Liu X L, Lin C C, Yuan S M. Blind dual watermarking for color images' authentication and copyright protection[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 28(5): 1047-1055

[152] Ahmadi S B B, Zhang G X, Rabbani M, *et al*. An intelligent and blind dual color image watermarking for authentication and copyright protection[J]. Applied Intelligence, 2021, 51(3): 1701-1732

[153] Aytekin Ç, Ozan E C, Kiranyaz S, *et al*. Extended quantum cuts for unsupervised salient object extraction[J]. Multimedia Tools and Applications, 2017, 76(8): 10443-10463

[154] Alshanbari H S. Medical image watermarking for ownership & tamper detection[J]. Multimedia Tools and Applications, 2021, 80(11): 16549-16564

[155] Sinhal R, Sharma S, Ansari I A, *et al*. Multipurpose medical image watermarking for effective security solutions[J]. Multimedia Tools and Applications, 2022, 81(10): 14045-14063

[156] Shen H, Chen B. From single watermark to dual watermark: a new approach for image watermarking[J]. Computers & Electrical Engineering, 2012, 38(5): 1310-1324

[157] Shi H, Li M C, Guo C, *et al*. A region-adaptive semi-fragile dual watermarking scheme[J]. Multimedia Tools and Applications, 2016, 75(1): 465-495

[158] Lei B Y, Zhao X, Lei H J, *et al*. Multipurpose watermarking scheme via intelligent method and chaotic map[J]. Multimedia Tools and Applications, 2019, 78(19): 27085-27107

[159] Al-Haj A, Amer A. Secured telemedicine using region-based watermarking with tamper localization[J]. Journal of Digital Imaging, 2014, 27(6): 737-750

[160] Priyanka, Maheshkar S. Region-based hybrid medical image watermarking for secure telemedicine applications[J]. Multimedia Tools and Applications, 2017, 76(3): 3617-3647

[161] Wu Nan, Lv Jianping. Dual watermarking algorithm based on DCT and DWT for color image[J]. Electronic Design Engineering, 2015, 23(23): 161-164(in Chinese)
(吴楠，吕建平. 基于 DCT 和 DWT 的彩色图像双功能水印算法[J]. 电子设计工程, 2015, 23(23): 161-164)

[162] Yu Xiaoqing, Li Hongchang, Zhang Mao. A multifunctional double-watermarking algorithm of color digital image for copyright protection and authentication[J]. Electronic Design

Engineering, 2012, 20(23): 32-35(in Chinese)
(虞晓庆, 李宏昌, 张茂. 兼具版权保护和内容认证彩色图像双水印算法[J]. 电子设计工程, 2012, 20(23): 32-35)

[163] Yu Xiaoqing, Li Hongchang, Zhang Mao. A multifunctional double-watermarking algorithm of colour digital image based on lifting wavelet[J]. Computer Applications and Software, 2013, 30(2): 50-53(in Chinese)
(虞晓庆, 李宏昌, 张茂. 基于提升小波的多功能彩色数字图像双水印算法[J]. 计算机应用与软件, 2013, 30(2): 50-53)

[164] Lan Xiamei, Li Hongchang. Dual watermarking algorithm of color image based on error-correcting codes[J]. Communications Technology, 2013, 46(11): 99-102(in Chinese)
(蓝夏梅, 李宏昌. 基于纠错编码的彩色图像双水印算法研究[J]. 通信技术, 2013, 46(11): 99-102)

[165] Sivananthamaitrey P, Murthy P S N, Kumar P R. Multifaceted watermarking of medical images using SWT and SVD[J]. International Journal of Advanced Science and Technology, 2019, 28(7): 1-14

[166] Hurrah N N, Parah S A, Loan N A, *et al*. Dual watermarking framework for privacy protection and content authentication of multimedia[J]. Future Generation Computer Systems, 2019, 94: 654-673

[167] Kumar S, Singh B K. DWT based color image watermarking using maximum entropy[J]. Multimedia Tools and Applications, 2021, 80(10): 15487-15510

[168] Zhao Y X, Zhou Z H. Multipurpose blind watermarking algorithm for color image based on DWT and DCT[C] //Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing. Los Alamitos: IEEE Computer Society Press, 2012: 1-4

[169] Kamili A, Hurrah N N, Parah S A, *et al*. DWFCAT: dual watermarking framework for industrial image authentication and tamper localization[J]. IEEE Transactions on Industrial Informatics, 2021, 17(7): 5108-5117