doi:10.3772/j.issn.1002-0470.2021.02.005

数字图像水印技术综述①

吴德阳②* 张金羽*** 容武艳** 唐 勇③* 赵 静* 曲长波***

(*燕山大学信息科学与工程学院 秦皇岛 066004)

(**广西中医药大学附属瑞康医院 南宁 530011)

(***辽宁工程技术大学软件学院 葫芦岛 125105)

摘 要 随着数字信息技术的快速发展,数字图像信息被广泛用于通信和信息的表示,但该类信息也常常会受到非法的篡改,因此如何保证数字图像的版权不被破坏是数字信息领域一直面临的问题。数字水印作为一种版权保护技术,能在一定程度上解决图像的版权纠纷问题,对数字图像技术的研究具有重要的意义。本文对近些年来国内外学者在该研究领域取得的成果进行了系统总结,首先给出了图像水印的基本模型、基本特性以及衡量指标;接着,分析了现有的数字图像水印算法特点,并进行分类,介绍了水印技术在其他领域的应用;然后,针对水印算法的抵抗行为,总结了现有水印算法能有效抵抗的鲁棒性攻击;最后,根据现有水印技术的优势和不足,提出未来的发展趋势和下一步研究的方向。

关键词 数字水印综述; 版权保护; 鲁棒性; 盲水印; 零水印

0 引 言

随着信息技术的飞速发展,数字信息的样式越来越丰富,如文本、音频、图像、视频等,使数据的存储和传输更加方便快捷,但许多违法分子经常使用图像编辑工具(例如 Potoshop、美图秀秀)对数字图像信息进行恶意篡改,导致原有的数字图像的版权得不到保证。同时图像作为通信交流中较为直观的信息,在日常生活中被广泛使用,如医疗图像、军事地图等[1-2]。如果图像内容被恶意修改或破坏,不但会失去图像原有的价值,同时也有可能引发版权纠纷,因此对于数字图像进行版权保护具有重要的意义。

数字水印作为一种版权保护技术[3],可以有效地解决版权保护和内容认证问题,其基本思想是通过嵌入算法将版权标识嵌入载体信息中,当发生版权纠纷时,通过嵌入算法的逆操作提取其中的版权信息,以确认图像的版权归属。然而,由于图像处理工具不断更新,给数字图像的版权保护带来了巨大的挑战,传统的加密方法,如数据加密算法(data encryption algorithm, DES)[4]、RSA[5]、Hash[6]等能在一定程度上保证图像信息的安全性,但这种加密方式只能防止图像信息不被使用,并不能保证信息的版权归属。数字水印技术可以很好地填补传统加密方法的不足,该技术可以将加密后的版权信息嵌入载体图像,既可以保证信息的安全性,同时在发生版权纠纷时又可以通过提取版权信息进行版权认证,因此对于数字图像的水印方法进行研究是非常有必要的。

基于文本或视频的数字水印算法通常选择将版权标识放在文本的表面[7-8],用于表明版权的归属。虽然这种版权保护方式能够清楚地显示版权标识,但不能很好保证信息的安全性,攻击者可以利用文

① 国家自然科学基金(61902340),河北省自然科学基金(F2018203060)和秦皇岛市科学技术研究与发展计划(201602A018)资助项目。

② 男,1992 年生,博士生;研究方向:版权保护,信息安全,计算机仿真;E-mail: wdy_ysu@126.com

③ 通信作者,E-mail: tangyong@ysu.edu.cn

(收稿日期:2020-01-22)

本或视频处理软件将表面的版权去除,同时可以将自己的版权信息添加到其中。这种非透明性的水印算法,在发生版权纠纷时,很难判断信息的版权归属。数字图像信息与其他文本信息不同,版权信息在嵌入过程中既要保证版权的透明效果,同时又不能影响图像的正常使用。为此现有的水印算法常常选择嵌入小容量的二值版权图像,虽然可以使载体图像获得很好的视觉效果,但是随着用户需求不断增大,选择彩色的 logo 作为版权信息会越来越受欢迎,因此在保证图像透明性的前提下,增大嵌入信息的容量,是数字图像水印领域面临的一项严峻挑战。

目前在数字图像方面的版权保护技术已有许多新颖的研究算法,但大多是基于一个方面的技术研究,缺乏对数字图像水印内容的系统认识。本文对近年来数字图像领域的新版权保护技术和算法研究进行梳理和分析,与其他文献相比,本文的主要贡献如下。

(1)梳理了自 2003 年以来国内外数字图像方面的数字水印文献,主要以 2010 年后的文献为主,详细讨论了数字图像水印领域的研究现状。

(2)系统地总结了数字图像水印领域常用的评价指标,并对图像方面的鲁棒性攻击进行分类、总结。

(3)更加全面地分析了现有数字图像水印算法优缺点,根据现有图像数字水印方面存在的问题,给出该领域未来更具发展潜力的研究方向。

本文第 1 节介绍了数字图像水印的基本模型、基本特性和评价指标;第 2 节对常见的图像水印算法进行分类,主要从特性、检测方法以及隐藏位置 3 个方面进行划分;第 3 节介绍了数字图像水印方面常见的攻击,并根据攻击特点划分为 3 类;第 4 节介绍了数字图像水印在其他领域的应用。第 5 节分析现有水印算法的优势和不足,对未来值得关注的研究方向进行了初步探讨。第 6 节总结全文。

1 研究框架

1.1 基本模型

数字图像水印技术是通过相应的水印嵌入规则将具有唯一性的版权标识嵌入到数字图像中,以达到信息隐藏的目的,并将版权标识注册到版权保护中心。当发生版权纠纷时,版权持有者可以通过水印提取算法提取版权标识,然后与注册到版权保护中心的水印图像进行比对,完成版权认证过程。

嵌入水印的基本模型如下:

$$I_w = I + \beta w \tag{1}$$

其中,I_w 为含有水印的图像,I 为原始载体图像,w 为水印图像,β 为缩放因子,控制嵌入水印的强度。

图 1 为数字图像水印的整体框架。由图 1 可以看出,该水印框架主要包含两个阶段,水印嵌入阶段和水印提取阶段。在嵌入阶段,水印信息需要先进行加密处理,以保证信息的安全性;而在提取水印时需要提供相应的密钥 k 才能提取完整的版权信息。

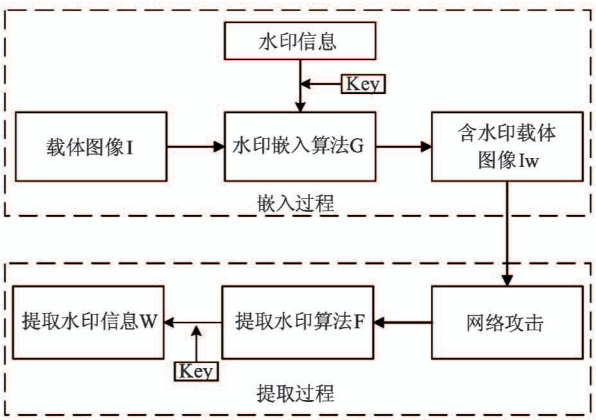


图 1 数字图像水印模型

1.2 基本特性

一个合格或者有效的水印算法需要满足一些特性才能保证系统的可靠性,但并不一定要求算法满足所有的特性。因为在提高算法一种特性的同时,另一种特性可能会受到影响,如文献[9,10]在透明性上具有较好的性能,最高的峰值信噪比可以达到 69.14,然而对于常见的攻击鲁棒性较差,提取水印图像的结构相似度只有 0.7011,但载体图像受到攻击后提取的版权图像仍能被识别出版权的归属。因此,需要在这些特性之间选择满足系统可靠性的平衡点,而数字图像水印的特性主要分为透明性、鲁棒性、虚警率和安全性。

透明性 透明性主要是指版权信息在嵌入载体图像过程中既不引起载体图像的明显变化,同时又能保证隐藏的信息在人类视觉系统下无法被识别出

来。用于提高数字图像透明性的方式主要有两种：一种是在载体图像中嵌入小容量的二值版权信息，如文献[11,12]，嵌入的信息大小仅为 32×32；另一种方式则是将版权信息嵌入能特征表示载体图像的最大奇异值中，如文献[13,14]，由于最大奇异值具有很好的稳健性，因此嵌入水印信息不会影响载体图像的视觉效果。

鲁棒性 鲁棒性主要是指含有版权信息的载体图像在经过网络噪声干扰或一定程度的篡改后，仍能从载体图像中提取清晰的版权图像。强鲁棒性一直是数字水印的难点，大多水印算法只能针对一种类型的攻击表现出强的鲁棒性，而对于其他攻击，效果则不佳。在现有文献中，用于提高算法鲁棒性的方法主要有离散小波变换(discrete wavelet transformation, DWT)[15]、曲波变换[16]和奇异值分解(singular value decomposition, SVD)[17]等。

虚警率 虚警率主要用于检测算法的可靠性。在完成信息隐藏后，通过用其他相似算法或者载体提取相似的版权信息，如果提取的信息与版权信息之间相似度高，则表明算法的虚警率较高，否则相反。尤其在零水印技术中为了降低虚警率，需要构造唯一性较强的载体特征，因此这一指标常用于衡量零水印的虚警率。

安全性 由于嵌有水印信息的载体图像需要在网络中传播，同时嵌入的算法通常是公开的，当载体图像被不法分子截获时，版权信息可能会被提取出来，进而导致算法失去了版权保护的目的，因此版权信息的安全性通常也是数字图像水印算法必需要具备的特性之一。在现有的图像水印算法中通过将版权信息进行置乱用于提高信息的安全性。常用的置乱方法主要有 Aronld 置乱[16]、混沌映射[17]、视觉密码[18-19]等，如文献[20,21]在嵌入版权信息之前，将版权信息进行置乱操作，由于 Aronld 置乱的周期性和混沌映射不可预测性，可以在一定程度上提高版权信息的安全性。

1.3 评价指标

评价一个水印算法的性能优劣，除了依靠人眼的视觉评价之外还需要一些客观性的衡量指标进行评价。数字图像水印算法现有的评价指标主要有归一化相关系数、峰值信噪比、结构相似度和误码率几种。

1.3.1 归一化相关系数

归一化相关系数(normalization cross correlation, NC)通常用于计算原始水印图像与被提取水印图像之间的相似性，取值范围为 $NC \in [0,1]$。当 $NC = 1$ 时，表示两个水印图像完全一致，表明算法的鲁棒性强；当 $NC = 0$ 时，表示两个水印图像无相关，NC 值的计算方式如下[22]：

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j)\times W'(i,j))}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j)]^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}[W'(i,j)]^2}} \tag{2}$$

其中，W 表示原始水印图像，W' 表示提取的版权水印，m 和 n 分别表示图像的长和宽。

1.3.2 峰值信噪比

峰值信噪比(peak signal to noise ratio, PSNR)通常用于衡量含水印载体图像与原始载体图像之间的失真程度，即水印图像的透明性，取值范围为 $PSNR \in [0,100]$。$PSNR$ 值越大，表明算法的透明性越好，否则相反，计算方式如下[23]：

$$MSE = \frac{1}{mn}\sum_{i}^{m}\sum_{j}^{n}[f(i,j) - g(i,j)]^2 \tag{3}$$

$$PSNR = 10\lg\left(\frac{MAX^2}{MSE}\right) \tag{4}$$

其中，f 表示原始的载体图像，g 表示含水印载体图像，MAX 表示图像像素的最大值。

1.3.3 结构相似度

结构相似度(structural similarity index metric, SSIM)用于计算两个图像之间的相似程度，取值范围为 $SSIM \in [0,1]$，$SSIM$ 值越大表示两个图像相似度越高，计算方式如下[24]：

$$SSIM = l(I,I')\times c(I,I')\times s(I,I') \tag{5}$$

$$\begin{cases} l(x,y) = \dfrac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \\ c(x,y) = \dfrac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \\ s(x,y) = \dfrac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \end{cases} \tag{6}$$

其中 C_1、C_2、$C_3 \in R^+$，μ_x 和 μ_y 分别表示图像 I 和 I' 的平均值，σ_x 和 σ_y 分别表示图像 I 和 I' 的协方差，σ_{xy} 表示两幅图像的协方差。

1.3.4 误码率

误码率(bit error rate,BER)表示图像中错误比特数据占总比特数据的比值,通常用于衡量水印算法的鲁棒性,但该衡量指标大都用于计算两幅二值版权图像之间的错误比特数,取值范围为 $BER \in [0,1]$,值越小反映算法的鲁棒性越好。具体计算方式如下[25]:

$$BER = \frac{b}{m \times n} \times 100\% \tag{7}$$

其中,b 为错误的比特数,$m \times n$ 表示图像的大小。

2 算法分类

随着对水印算法的深入研究,近年来提出了许多优秀的数字图像水印算法,在现有的研究基础上,本文将数字图像水印划分方式分成 3 大类。按特性划分可以分为鲁棒水印、脆弱水印;按检测方式划分可以分为盲水印、非盲水印、零水印;按隐藏位置划分可其分为基于频域的水印算法和基于空域的水印算法,具体划分方式如图 2 所示。

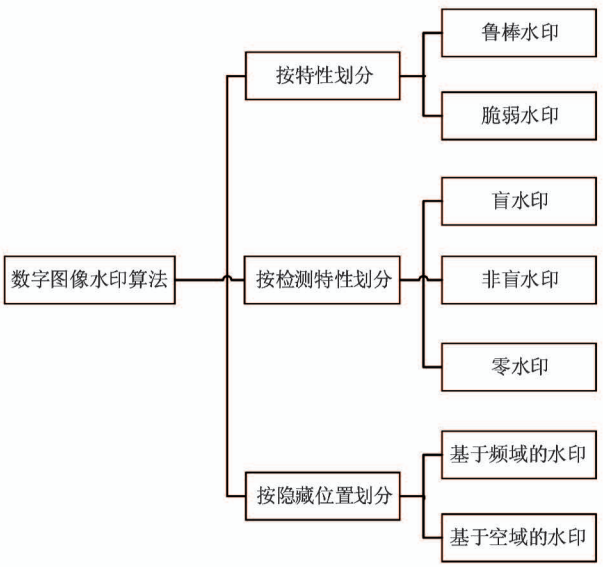


图 2 数字图像水印算法分类

2.1 按特性划分

2.1.1 鲁棒水印

鲁棒水印是指将作品创建者或持有者的版权标识嵌入到载体信息中,含有版权信息的载体经过一般的图像处理操作(噪声、滤波、锐化等),或部分恶意攻击后仍能提取完整的版权信息。在鲁棒水印算法中,如何提高算法鲁棒性是主要考虑的问题,现阶段的鲁棒水印算法常常使用小波变换、离散小波变换等频域变换与奇异值分解、正交三角分解(orthogonal-triangular decomposition,QR)等矩阵分解工具来去除图像信息中冗余且敏感的信息,以抵抗常规的图像处理操作。因此基于频域变换水印算法也包含在鲁棒水印算法的范畴,如文献[13,14]利用奇异值分解获得图像每一子块的最大奇异值为

$$\boldsymbol{I} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}} = \boldsymbol{U}\begin{bmatrix} \lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,n} \end{bmatrix}\boldsymbol{V}^{\mathrm{T}} \tag{8}$$

其中,$\boldsymbol{U}$ 表示左奇异矩阵,$\boldsymbol{V}$ 表示右奇异矩阵,λ 表示奇异值,n 表示矩阵大小。由于最大奇异值在受到常规图像处理后变化较小,因此能够提高算法的鲁棒性。借鉴文献[13,14]的思想,陈青等人[26]改变原有奇异值分解的过程,提出双奇异值分解的鲁棒水印算法。双奇异值分解除了保持传统奇异值分解特性之外还增加了更多的秘钥矩阵,提高算法的安全性。由于小波变换具有多尺度和局部表征的特性,即使载体图像受到一般的图像处理,小波变换、奇异值分解也能提取载体的局部特征,这种局部表征能力和旋转不变性可以有效削减噪声、滤波、旋转等攻击对载体图像的影响,进而保证了水印信息的完整性和安全性。

2.1.2 脆弱水印

与鲁棒水印相比,脆弱水印常用于判断数字内容是否被篡改,并在不参考原始数字内容的情况下将篡改区域与未篡改区域区分开来[27],在保护信息的完整性和安全性方面具有重要意义。如李赵红和侯建军[28]在离散余弦变换(discrete cosine transform,DCT)域提出混沌脆弱水印,该算法根据 DCT 域高频信息的敏感性,将经过混沌映射后的水印信息嵌入高频信息中,可以得到很好的篡改定位能力,同时在版权认证阶段实现了盲检测,但该方法无法定位在滤波攻击和 JPEG 压缩攻击后的图像篡改位置。为此 Rawat 和 Raman[29]在文献[28]的基础上,

提出一种新的脆弱水印算法，经两次混沌映射后将水印信息嵌入载体图像的最低有效位中，由于混沌映射对初值敏感，因此，当使用错误的秘钥提取版权信息时，可以准确地定位篡改位置。Azeroual 和 Afdel[30] 利用 Faber-Schauder 小波变换（Faber-Schauder discrete wavelet transform，FSDWT）对最低有效位（least significant bit，LSB）进行变换，为了使水印算法更加脆弱，对 FSDWT 后的图像进行分块处理并选择子块的最大系数，最后将系数与版权水印进行异或处理。该算法将利用 FSDWT 系数生成的水印嵌入到原始图像的 LSB 中，对篡改区域进行准确定位。Zhang 等人[31] 利用奇异值分解后左、右奇异值矩阵的关系提出一种脆弱水印算法，该算法与 Azeroual 等人的方法不同，该算法直接对载体图像的每一子块进行奇异值分解，并根据左、右奇异值矩阵的第一列的乘积构造二值特征矩阵，最后将该特征矩阵嵌入载体图像的最低有效位中。侯翔等人[32] 利用坐标网格分块的矢量地图脆弱水印算法对地图进行分块时，利用地图的地理坐标进行划分，这种分块方式保证了地图坐标信息的完整性。为了防止数据点溢出而造成数据认证失败，该算法通过修改数据点与子块边距的最短距离来确保数据点保留在数据子块中，相比传统的认证方法，具有很好的稳定性和定位精度。

2.2 按检测方式划分

2.2.1 盲水印

盲水印的基本思想是将版权水印的整体信息量化地嵌入到载体图像中，并且在检测水印信息时，不需要提供原有水印的任何信息即可完成水印的提取过程。盲水印嵌入模型如下：

当 $W_{i,j}=1$ 时，有

$$\lambda=\begin{cases}\lambda-T_{i,j}-\delta/4 & T_{i,j}\leqslant\alpha/4\\ \lambda-T_{i,j}+3\times\alpha/4 & \text{其他}\end{cases} \tag{9}$$

当 $W_{i,j}=0$ 时，有

$$\lambda=\begin{cases}\lambda-T_{i,j}+5\times\alpha/4 & T_{i,j}\geqslant 3\times\alpha/4\\ \lambda-T_{i,j}+\alpha/4 & \text{其他}\end{cases} \tag{10}$$

式中，$T_{i,j}=\mathrm{mod}(\lambda_{i,j},\alpha)$，$\lambda$ 表示最大奇异值，α 为最大量化参数，$W_{i,j}$ 为二值水印中的像素值。由于盲水印便捷、实用的特性，因此被广泛使用于图像的版权保护。如文献[33]利用 DWT 和 SVD 来获取载体图像的最大奇异值，然后对奇异值矩阵的后 7 位进行循环移动，将水印信息嵌入到载体图像的亮度分量中。该方法对于小尺度的剪切攻击具有较好的抵抗性能，但提取的水印图像含噪声点较多。Thanki 等人[34] 利用 Curvelet 变换获得载体图像的高频 Curvelet 系数，然后利用冗余离散小波变换（redundant discrete wavelet transform，RDWT）将水印信息分别嵌入每子块的 RDWT 中。由于 Curvelet 变换对于图像的曲线特性表现性较强，同时 RDWT 采用非下采样机制对图像进行变换，可以有效地保证图像的平移不变性，因此克服了小波变换下采样后小波系数变化较快的不足。

盲水印的最大缺点是对于剪切攻击提取的水印会出现局部缺失的现象，如文献[35-37]提出的盲水印算法，在图像的剪切位置出现了水印局部缺失现象。由于载体图像受到剪切攻击时，载体图像的局部低频信息被置为零，因此提取的版权水印在局部出现缺失的现象。这种局部缺失现象对于普通的水印版权标识影响较小，但对于以二维码作为版权图像的水印算法而言，可能会造成版权信息无法读取的情形。如 Li 和 Cui[38] 提出一种基于 QR 码的盲水印算法，在剪切攻击下无法提取完整的水印信息。为了克服盲水印在几何攻击方面的缺点，文献[39,40]提出了一种抗几何攻击的盲水印算法。文献[39]利用 Directionlet 变换的倾斜式各向异性，构造水印的同步信息，并直接以图像边缘的方向为参考方向将水印嵌入，由于选取的边缘斜率不易发生变化，因此在受到攻击时，抗几何性能较强。与文献[39]不同，文献[40]则利用尺度不变特征变换（scale invariant feature transform，SIFT）变换对受到攻击后的图像进行校正，在图像旋转 45 °时，得到的 *NC* 值高达 0.9980。表明这种策略能够很大程度地提高算法的抗几何攻击性能。

综述分析，盲水印主要存在以下几个优势。

（1）盲水印通过量化器选择与原始载体数据最接近的数据代替原始的载体数据，因此具有较好的保真度。

(2)盲水印提取水印的过程属于盲提取方式,因此在进行版权认证时不需要提供任何版权信息即可完成水印的提取过程,认证便捷、实用。

2.2.2 非盲水印

非盲水印是指在提取版权信息时需要用户提供水印的另一部分信息才能完成提取水印信息的过程。与盲水印不同,非盲水印只是将水印图像的特征信息嵌入载体图像中,即使载体图像受到攻击,只对部分水印信息造成影响,因此,与盲水印相比鲁棒性会更好,其模型如式(11)~(13)所示。

$$[\boldsymbol{U}\ \ \boldsymbol{S}\ \ \boldsymbol{V}] = svd(\boldsymbol{I}) \tag{11}$$

$$[\boldsymbol{u}\ \ \boldsymbol{s}\ \ \boldsymbol{v}] = svd(\boldsymbol{w}) \tag{12}$$

$$\boldsymbol{S}' = \boldsymbol{S} + \alpha \times \boldsymbol{s} \tag{13}$$

式中 svd 为奇异值分解操作,$\boldsymbol{I}$ 为载体图像,$\boldsymbol{w}$ 为水印图像,$\boldsymbol{U}$、$\boldsymbol{S}$、$\boldsymbol{V}$ 和 $\boldsymbol{u}$、$\boldsymbol{s}$、$\boldsymbol{v}$ 分别表示载体图像与版权水印的左奇异矩阵、奇异值矩阵、右奇异矩阵,$\boldsymbol{S}'$ 为嵌入水印信息后的奇异值矩阵,α 为嵌入强度。由非盲水印的模型可以看出,嵌入过程只是将水印的奇异值嵌入到载体图像的奇异值中,因此在提取版权水印时,需要提供原始水印的左奇异值矩阵 $\boldsymbol{U}$ 和右奇异值矩阵 $\boldsymbol{V}$,该类水印算法认证过程比较繁琐,实用性能较差。

文献[41-43]利用小波变换后低频信息的稳定性和奇异值分解的健壮性,将版权信息嵌入载体图像的低频域中。由于小波变换对于高频信号(如噪声)具有很好的过滤作用,因此在常见的非几何攻击方面表现出强的鲁棒性,但在几何攻击方面,像素位置发生较大的变化,小波系数影响较大,抵抗性能较差。同时块最大奇异值虽然能表示一个子块的能量信息,但当载体图像局部位置的像素被剪去时,块奇异值从最大值变成 0,此时无法表达图像子块的信息。

由于奇异值分解在大强度的几何攻击下存在较大的波动性,为此文献[44,45]利用 SIFT 进行几何校正以提高算法在几何攻击方面的性能。文献[44]得到的 NC 值均在 0.9932 以上,而对载体图像进行放大 2 倍时,NC 值仍能达到 0.9751。文献[45]先将载体图像进行非下采样轮廓波变换(nonsubsampled contourlet transform,NSCT)变换获得低频信息,然后利用 SIFT 来提取载体图像的特征点,最后将水印信息嵌入低频信息中,对于常见的几何攻击和组合攻击具有较强的抵抗能力和顽健性。SIFT 特征点的最大优势是在载体图像的像素位置或者局部缺失时,仍能提取稳定的特征点,因此在抗旋转攻击、缩放攻击和剪切攻击上性能要优于传统的奇异值分解。

2.2.3 零水印

虽然鲁棒水印和盲水印在鲁棒性上具有很好的优势,但嵌入式水印方法大都存在鲁棒性与透明性之间的矛盾。版权水印嵌入载体图像时,不仅对透明性造成一定影响,同时还会破坏原有图像的数据结构,而对于要求内容完整性较高的信息,鲁棒水印和盲水印很难满足这种需求。

基于鲁棒水印和盲水印在内容完整性和透明性上的不足,温泉等人[46]提出了零水印的概念,其基本思想是通过提取载体图像的特征与版权水印生成具有唯一性的零水印信息,最后将生成的零水印信息注册到版权保护中心,其模型如图 3 所示。由图 3 可看出载体图像构造的特征一般为二值特征矩阵,其目的是为了便于与二值版权水印进行逻辑运算,同时生成的零水印通常是杂乱无章的二值信息,因此生成零水印有利于提高信息的安全性。在发生版权纠纷时,只需要将生成的零水印与受攻击后的图像特征进行逻辑运算即可,这种认证方式相比盲水印和鲁棒水印更便捷。

由于零水印解决了嵌入式水印鲁棒性与透明性之间的矛盾,因此被广泛用于数字图像的版权保护[47-49]。根据零水印构造的特征矩阵可以将零水印算法划分为基于频域变换的零水印和基于空域的零水印。基于频域的零水印通过利用 DCT、DWT、Curvelet 变换和主成分分析(principal component analysis, PCA)[50]等变换工具将图像从空间域变换成频率域信息获取载体图像的低频信息,然后再利用奇异值分解构造载体图像的特征矩阵。如 2014 年 Prathap 等人[51]利用 Contourlet 变换提取载体图像的低频信息,并通过 PCA 构造特征信息,在非几何攻击上具有较强的鲁棒性。而另一种策略则是结合密码学原理生成零水印,如曲长波等人[52-53]提出

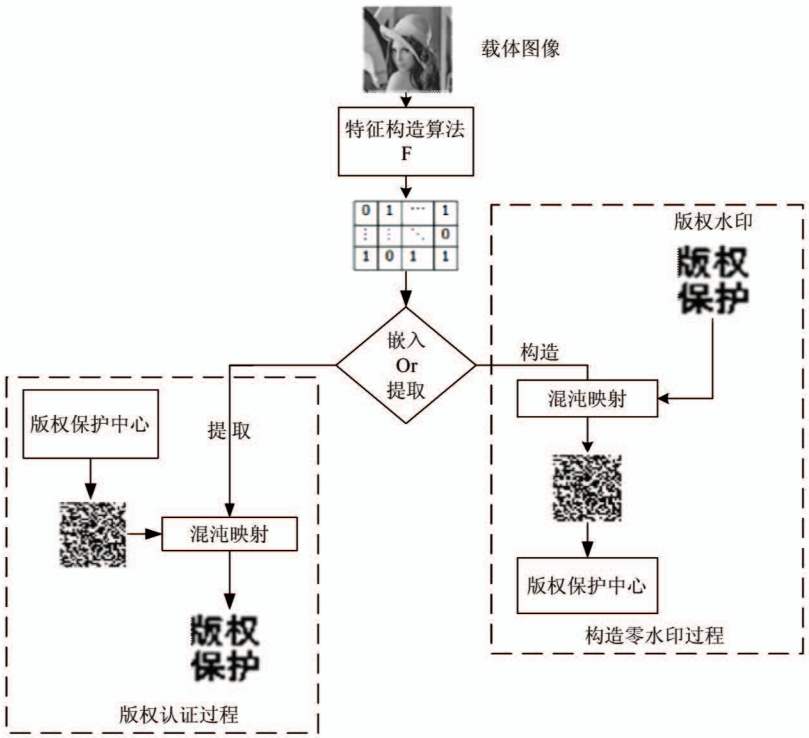


图 3　零水印模型

的视觉密码零水印算法、文献[52]通过利用视觉密码原理得到零水印信息，在小尺度的攻击上具有较强的鲁棒性。而文献[53]则利用视觉密码处理版权图像，将版权图像一分为二，只用其中一个密钥图份与特征矩阵生成零水印信息，而另一密钥图份则用于版权认证过程，该算法特点在于版权信息安全性较高。

基于频域变换的零水印算法需要频繁的时-频变换，增加了算法的复杂度。为此廖琪男[54]直接在图像的空域上构造了一种基于几何校正的零水印，并利用 SIFT 对旋转后的图像进行校正，在噪声攻击、旋转攻击上获得较好的鲁棒性，但其在抵抗 JPEG 压缩上的性能不佳。基于此，2017 年熊祥光[55-56]提出了空域鲁棒零水印算法，该算法直接在空域上利用图像的整体均值与各个子块均值之间的关系构造特征矩阵，由于整体均值与各个子块的矩阵均值是成正比关系，因此对于非几何攻击，表现出强的鲁棒性。综上分析，零水印具有以下优点。

（1）透明性好。由于零水印不需要将版权信息嵌入载体图像，因此在透明性和内容完整性上，该类算法具有独特的优势。

（2）安全性高。零水印算法生成的零水印为唯一性强且杂乱无章的图像信息，即使被截获也无法识别出真正的版权信息，即零水印产生过程等价于对版权信息进行二次加密操作，因此安全性更高。

2.3　按隐藏域划分

2.3.1　基于频域的水印算法

基于频域变换的水印算法是将图像的空间域转换成频率域，然后根据嵌入水印的需求提取低频子带，并将水印嵌入载体图像的低频域中。由于载体图像的低频信息具有较好的隐蔽性能，因此大多数算法都选择将水印嵌入载体图像的低频域中，如文献[57]利用 DCT 对每一子块进行变换获取能量集中的低频系数，将水印信息嵌入每一子块的低频系数中，然后通过 DCT 的逆变换完成水印的嵌入。由于 DCT 属于一种线性变换工具，因此具有极强的能量压缩特性，但其变换过程是将载体图像的整体空间域变换成频率域，属于一种全局变换操作，不具备局部变换特性，因此在处理局部突变信号时能力较差。

针对 DCT 的不足，文献[58]提出了小波和交叉小波树的盲水印水印算法，利用离散多小波对载体

图像进行三级小波分解,获得 LL3 低频子带,然后根据能量系数将水印嵌入载体图像中。由于 DWT 能够将图像信号划分成不同的频段信息特性,因此 DWT 的这种局部特性能够很好地克服 DCT 不能进行局部划分的缺点,并且能够很好地解决信号突变的问题。文献[59,60]提出一种对直线特征具有较高逼近精度和稀疏表达性能的脊波(Ridgelet)变换水印算法,其将子块内的曲线特征用脊波的直线特性进行逼近,并对每一子块进行 SVD,构造载体图像的特征矩阵。与 DWT 不同,脊波变换需要将图像进行 Radon 变换[61],然后再利用一维 DWT 变换提取低频系数,经过 Radon 变换后的频域系数为特定方向、特定截距上原图像所有像素点的灰度值的叠加,因此,相比之下,脊波变换在频域变换中增加了方向的选择,在构造的特征中保留了丰富的图像特征信息。

虽然 Ridgelet 变换在直线逼近方向上较 DWT 更有优势,但是 Ridgelet 变换很难逼近图像中的曲线奇异特性,如果用直线去刻画图像的曲线边缘信息,其逼近性能如同 DWT 一样。因此,为了使构造的特征矩阵包含更多的图像曲线特征,2011 年石慧等人[62]将载体图像进行 Contourlet 变换,然后在不同方向的子带中选择重要系数作为水印嵌入的位置,由于充分利用 Contourlet 的多尺度、局部化、方向性的特性,因此在抵抗旋转、翻转、缩放等几何攻击上具有很好的鲁棒性。2012 年 Bazargani 等人[63]比较了基于 DWT、Curvelet、Contourlet 变换的鲁棒性能。实验结果表明,基于 Contourlet 域的水印算法在抵抗噪声、滤波、旋转、缩放攻击上鲁棒性都优于基于 DWT 的水印算法,然而对剪切攻击的抵抗能力要差。主要原因是 DWT 局部特性只考虑图像的近似方向的信号,而 Curvelet 和 Coutourlet 得到的近似分量包含其他方向的能量值最大的信息,因此,在局部剪切时,Curvelet 和 Contourlet 丢失的信息要比 DWT 的大。为了克服 Contourlet 变换最后一层低频子带没有被划分的缺陷,2017 年鲁荣波等人[64]提出 Contourlet 域虚拟树结构的概念,通过计算每棵虚拟树的均方差选择水印嵌入位置,同时利用果蝇算法[65]优化支持向量回归机[66]的参数,最后利用 SVR 自适应地将水印信息嵌入载体图像,该方法与类似的水印算法相比,透明性和鲁棒性都比较好。

2.3.2 基于空域的水印算法

虽然基于频域变换的水印算法在透明性和抵抗噪声、滤波等攻击上具有很好的优势,但这类算法设计往往较为复杂,与频域变换的水印算法不同,基于空域的水印则不需要将空间域信息转换成频域信息,其基本思想是直接将水印信息嵌入载体图像的不可见区域,如最低有效位(LSB)[67]。由于 LSB 的变化不会影响图像的视觉效果,但 LSB 允许嵌入的水印信息容量较小,同时载体图像受到噪声干扰时,LSB 的抗鲁棒性差。为此,Zhang[68]提出了基于 SVD 分解的空域水印算法,该算法将预处理后的水印信息量化嵌入载体图像奇异值中,对于左上角剪切得到 *NC* 值仍为1.0000。2018 年曲长波等人[69]提出一种空间彩色水印算法,该方法有两个优点,其一是不需要进行频域变换,且能抵抗较大强度的鲁棒攻击;其二是利用彩色版权标识构造了彩色的零水印,相比传统的二值零水印安全性更高,且信息表达更丰富。2019 年 Abraham 和 Pual[70]提出高透明性的空域水印算法,该方法将水印嵌入彩色图像的蓝色分量中,由于彩色图像具有 24 位的容量信息,当其中一个颜色分量发生改变时,对于彩色载体图像的影响较小,因此,嵌入在其中的水印信息具有较好的隐蔽性。

根据对以上文献中算法的分析,各种算法所采用的技术以及优缺点如表 1 所示。针对表 1 中给出的水印算法的特点,总结出数字图像水印关于所使用技术和版权信息的整体脉络如下。

(1)从技术特点来看,大部分算法都选择 DWT 及其改进技术作为频域变换工具,主要由于小波变换所分解的低频信息能够有效提高算法的鲁棒性,同时结合 SVD、QR 分解使得算法在抵抗几何攻击方面具有很好的性能。

(2)从所使用的水印图像类型来看,现有的水印算法大都使用大小为 64 × 64 的二值图像作为版权信息,主要由于嵌入较小的版权信息不会破坏图像的视觉效果。

(3)从算法类型来看,非盲水印相比于盲水印

算法、鲁棒水印算法、脆弱水印算法、零水印算法嵌入的水印信息更大，主要由于非盲水印只嵌入了部分水印信息，因此提取信息时，需要额外的水印信息，这也是非盲水印的不足之处。

(4)从算法的优缺来看，不同类型的水印算法都拥有各自的特点，这主要取决于算法的用途，如脆弱水印与盲水印相比，脆弱水印主要侧重于篡改位置的准确定位，而盲水印则侧重于受攻击后的信息盲检测的过程。对同一种类型的水印技术的不同水印算法，主要考虑鲁棒性与透明性，如一些算法虽然能抵抗大角度的旋转攻击，但透明性较差。

表 1 水印技术算法分析

水印技术	文献	技术特点	优点	缺点	水印类型(大小)
鲁棒水印	[13]	DWT、SVD	安全性、鲁棒性好，尤其对于抗旋转攻击	抗剪切能力差，版权认证过程繁琐	二值水印(64×64)
	[26]	双奇异值分解，小波变换	抗噪声、滤波、旋转攻击	---	---
脆弱水印	[28]	DCT 变换，Logistic 混沌映射	算法简洁，篡改定位准确	抗鲁棒性攻击能力弱	二值水印(4×4)
	[29]	Arnold 置乱、Logistic 加密、LSB 最低有效位	安全性和鲁棒性好	无法定位在滤波攻击和 JPEG 压缩攻击后的篡改位置	二值水印(256×256)
	[30]	Faber-Schauder、DCT，LSB 最低有效位	篡改定位准确，实时	---	二值水印(64×64)
盲水印	[33]	DWT 和 SVD	抗小尺度非几何攻击性能好	无法抵抗旋转攻击	二值水印(32×32)
	[34]	DCuT 和 RDWT	计算速度快、透明性好	抗大角度旋转攻击和滤波攻击差	二值水印(64×64)
非盲水印	[39]	Directionlet 变换	抗几何攻击性能好	---	二值水印(64×64)
	[44]	小波变换、SIFT 校正	抗几何攻击能力强	---	二值水印(64×64)
	[45]	NSCT 变换，SIFT 校正	抗旋转攻击能力强	抗剪切攻击鲁棒性差	二值水印(16×16)
零水印	[51]	Contourlet 变换、PCA	对几何攻击和非几何攻击都表现出强鲁棒性	对缩放攻击无法提取清晰版权信息	---
	[53]	Curverlet 变换、SVD、视觉密码	鲁棒性和安全性都比较好	算法设计较为复杂	二值水印(64×64)
	[55-56]	子块均值与整体均值之间的关系	对于非几何攻击，表现出强的鲁棒性	无法抵抗剪切攻击和旋转攻击	二值水印(64×64)

注： ---表示无此项

3 攻 击

水印攻击方式包括鲁棒性攻击、表示攻击以及解释攻击等。鲁棒性攻击是最常见的攻击手段，也是最有效的检验手段。表示攻击可以让检测器检测不到水印的存在。解释攻击与鲁棒性攻击原理相反，利用水印技术的逆方法伪造水印，以达到伪造水印的所有权的目的。

3.1 鲁棒性攻击

鲁棒性攻击是常用于检验算法的有效手段之

一,嵌入水印信息的图像可能被人为篡改或网络攻击,破坏提取水印算法的同步性,因此水印算法在设计完成之后,需要进行相应的攻击实验。根据攻击的性质可以将图像攻击分为三类,即非几何攻击、几何攻击和组合攻击。

3.1.1 非几何攻击

非几何攻击是对图像像素进行微小的篡改或者添加干扰值,该类攻击主要以削弱信号强度为主,常见的非几何攻击主要包含噪声攻击、滤波攻击、JPEG 压缩攻击,具体攻击类型分类如图 4 所示。

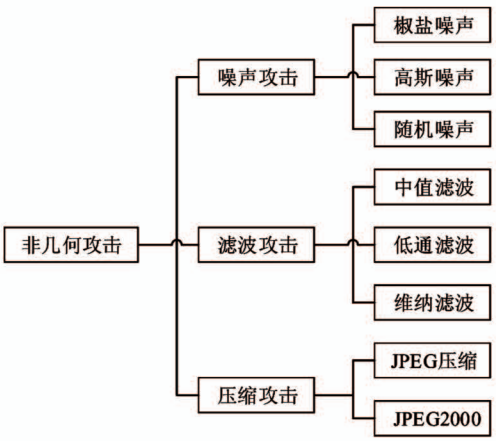


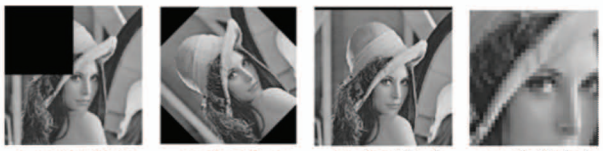
图 4 非几何攻击分类

如图 4 所示,同一种攻击可包含 2 种及以上的攻击类型。一种攻击中的不同类型对水印的鲁棒性影响也不同,例如噪声攻击中的高斯噪声,其噪声点服从高斯分布,对于某个强度的噪声点比较集中,强度较大,因此对水印的清晰度影响较大;而椒盐噪声可表示为一种逻辑噪声,其特点是噪声分布如同在图像表面撒上的椒盐,使得图像出现黑白斑点,一般对算法的影响较小。

3.1.2 几何攻击

几何攻击主要是指破坏水印嵌入和提取的同步性,该类攻击通过改变图像的原始像素位置来达到破坏水印的效果。几何攻击相比非几何攻击对图像的影响更大,由于其通过遮挡、移动和旋转等操作改变图像像素的局部或整体位置,在提取水印时,如果仍按原始像素位置进行提取,则会导致版权信息提取不全或无法提取的情形。常见的几何攻击如图 5 所示。

由图 5(a)可以看出,剪切攻击的特点是使载体图像的局部位置的像素为 0,属于局部攻击操作;如图 5(b)所示,旋转攻击的特点是使图像的整体像素位置发生改变,同时旋转过程中伴随着剪切操作,因此该种攻击对水印的破坏性比较大;行列偏移攻击只是将图像的整体像素向上下移动,被移动后位置用 0 进行填补,如图 5(c)所示;缩放攻击则是将图像进行放大或缩小,如图 5(d)所示。



(a) 剪切攻击 (b) 旋转攻击 (c) 行列偏移 (d) 缩放攻击

图 5 几何攻击分类

3.1.3 组合攻击

数字信息在复杂的网络中传输常常受到多种类型的攻击,如非几何攻击 + 非几何攻击、几何攻击 + 非几何攻击、几何攻击 + 几何攻击等组合类型的攻击。该种攻击类型除了影响载体图像的像素值之外,还会改变图像几何结构,对信息具有很大的破坏性。

3.2 表示攻击

表示攻击的目的是为了使侵权检测器不能检测到水印的存在。通常使用较小的水印图像避免检测器的检测以达到“逃避”检测的目的。表示攻击利用这一特点,将水印图像分割成细小的碎片,使检测器无法检测到水印,导致难以确定信息的所有权。其不会破坏原图像,只是将原始图像进行分割,在版权认证时,可以将各个子块水印信息进行拼接即可恢复原始信息。

3.3 解释攻击

解释攻击是利用水印的逆算法,将想要的水印嵌入到原图像中,并保证原图像的透明度。这样伪造出来的水印信息与原水印算法得到水印信息很相似,因此很难辨别出图像的所有权。但解释攻击需要知道原水印算法的细节和嵌入方式,以便伪造出假的水印和虚拟的原图像。这种攻击的预防方式就是构造出不可逆的水印算法或者不可逆的哈希过程。同时也可以建立一个可靠的第三方水印验证机

构,来保护水印信息的所有权,增加数字水印技术的安全性。

4 其他应用领域

近年来,随着对水印技术的深入研究,水印技术也被广泛应用于其他特殊数字图像领域,如医疗图像、遥感图像、数字地图等。由于这些数字图像的结构与常见的数字图像不同,因此对原始信息内容完整性和透明性的要求较高。

4.1 医疗领域

医疗图像主要分为 B 超图像、X 照片、CT 影像等,这类数字信息常常包含一些重要的疾病信息,为医生疾病诊断提供重要依据。如果医疗信息受到恶意篡改,将会影响医生的判断,因此如何保证医疗信息的完整性和安全性是医学图像领域一直面临的挑战。为了防止医疗数据被恶意修改,通常需要对其进行有效的身份验证。如文献[71,72]提出了一种鲁棒的非盲医学图像水印方案,对图像执行 I 级分数阶小波变换(fractional wave packet transform,FRWPT),并将水印嵌入修改后的参考图像中,通过测试发现,这种方法在乳腺 X 线照片上的测试结果具有较好鲁棒性。

4.2 遥感领域

遥感影像主要用于实时监测和统计调查。由于其信息的敏感性特点,对其进行版权保护时需要考虑到遥感地图的透明性和完整性。Jiang 等人[73]提出了一种应用于遥感影像的基于加密的水印技术,利用正交分解系数不变性原理和 DCT 变换将水印信息嵌入载体图像的低频部分,该算法在抵抗非几何攻击上具有强的鲁棒性。Li 等人[74]提出了一种基于四元小波变换(quaternion wavelet transform,QWT)和张量分解的非盲水印算法,QWT 方法可以更好地保留图像特征,应用于彩色遥感图像上可以获得更好的透明性。Tong 等人[75]提出了一种应用于遥感图像的改进的压缩感知水印算法,采用提升小波变换、Hadamard 矩阵和三元水印序列来提高算法的鲁棒性,并取得了良好的效果。

4.3 地图版权方面

随着时代的不断发展和进步,地图的应用范围越来越广泛。例如,百度地图、谷歌地图中用到的平面地图实质上就是二维矢量地图,由于地图往往包含一些坐标、位置、方向等信息,因此该类数字图像的版权保护主要考虑地图信息的透明性和安全性。文献[75]提出了一种基于可逆对比度映射的二维向量图可逆水印算法,它首先选择顶点的坐标并根据数据精度要求选出可以嵌入水印的位置,使用可逆对比度将加密水印嵌入到选出的相对坐标中进行映射转换。嵌入水印后的地图坐标信息与原始信息一致。

5 研究不足与未来趋势

根据对现有研究成果的分析,总结了该领域存在的问题及未来发展面临的挑战。

(1)基于彩色版权图像的水印算法

现阶段的图像水印算法所使用的版权图像大都为二值的版权标识,虽然有利于图像的保真性,但是随着图像信息的快速发展和拍照设备的更新,客户对于多样性的图像需求和彩色图像使用需求越来越大,因此将彩色的 Logo 作为版权水印,对于图像的保真度是一项严峻的挑战。

(2)面向人工智能的水印算法

图像水印技术发展至今,很大部分算法仍在使用传统的方法和工具对图像信息进行版权保护,然而随着图像软件的日益更新,传统的图像加密方法对于现有的攻击方式难以保证版权信息的鲁棒性和清晰度。同时,近年来,人工智能、深度学习技术在图像处理领域上具有较强的优势,通过深度学习技术学习训练常见的攻击方式,然后对受攻击后的载体图像进行“修补”,实现智能水印嵌入、攻击检测、以及智能水印提取,对于抵抗鲁棒攻击具有更大的作用。

(3)多领域结合的水印算法

数字水印的重要指标之一就是保证版权信息的安全,然而现有算法大多侧重于鲁棒性和透明性,对于水印的安全性研究较少,因此,未来数字水印技术与密码技术相结合能够使版权保护更好地应用于复杂的网络环境。

(4)高效的水印算法

高透明性和强鲁棒性一直是水印算法的两个重要指标,然而随着图像尺寸不断增大,在水印的嵌入和提取过程中,需要花费更多的时间进行矩阵运算。多核并行处理器的引入,能够高效地解决大矩阵运算的效率问题,因此,在数字图像水印技术中利用GPU的并行计算特性能够提高嵌入和提取水印的时间效率。

6 结 论

近年来,数字信息的版权保护越来越受到人们的关注,尤其在数字图像领域,图像信息的版权保护和安全性更是人们重点关注的信息之一。本文主要围绕数字图像方面的水印算法和研究现状进行了梳理、分类,总结了数字图像水印算法的优势与不足,列举了几种水印攻击方式,并阐述了预防方法。对比分析了小波变换相关的技术,总结了各种水印技术的模型公式,尤其重点讨论了零水印的原理及其优缺点。这为后续的研究提供了重要的参考依据,对数字图像版权保护技术的发展起到一定的推动作用。

参考文献

[1] Thanki R, Borra S, Dwivedi V, et al. An efficient medical image watermarking scheme based on FDCuT-DCT[J]. *Engineering Science and Technology, an International Journal*, 2017, 20(4): 1366-1379

[2] 李旭东. 抗亮度和对比度攻击的DCT域图像数字水印算法[J]. 光电子·激光, 2013,24(6):1184-1190

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

[4] Zhang Y P, Liu W, Gao S P, et al. Digital image encryption algorithm based on chaos and improved DES[C]//2009 IEEE International Conference on Systems, Man and Cybernetics, San Antonio, USA, 2009: 474-479

[5] Nadiya P V, Imran B M. Image steganography in DWT domain using double-stegging with RSA encryption[C]// 2013 International Conference on Signal Processing, Image Processing and Pattern Recognition, Coimbatore, India, 2013: 283-287

[6] Norouzi B, Seyedzadeh S M, Mirzakuchaki S. A novel image encryption based on Hash function with only two-round diffusion process[J]. *Multimedia Systems*, 2014, 20(1):45-64

[7] Qi W F, Yang G Y, Zhang T, et al. Improved reversible visible image watermarking based on HVS and ROI-selection[J]. *Multimedia Tools and Applications*, 2019, 78(7): 8289-8310

[8] 赵星阳, 孙继银. 一种可抗二值化攻击的文本图像可见水印算法[J]. 计算机应用, 2009, 29(1):165-167

[9] Arora S M. A DWT-SVD based robust digital watermarking for digital images[J]. *Procedia Computer Science*, 2018, 132: 1441-1448

[10] Moosazadeh M, Ekbatanifard G. An improved robust image watermarking method using DCT and YCoCg-R color space[J]. *Optik-International Journal for Light and Electron Optics*, 2017, 140:975-988

[11] Zhang H, Shu H, Coatrieux G, et al. Affine legendre moment invariants for image watermarking robust to geometric distortions[J]. *IEEE Transactions on Image Processing*, 2011, 20(8):2189-2199

[12] 朱新山, 陈砚鸣, 董宏辉, 等. 基于双域信息融合的鲁棒二值文本图像水印[J]. 计算机学报, 2014, 37(6):1352-1364

[13] Nguyen T H, Duong D M, Duong D A. Robust and high capacity watermarking for image based on DWT-SVD[C]// The 2015 IEEE RIVF International Conference on Computing and Communication Technologies-Research, Innovation, and Vision for Future (RIVF), Can Tho, Vietnam, 2015: 83-88

[14] 肖振久, 李南, 王永滨, 等. 基于Contourlet奇异值分解的强鲁棒数字水印算法[J]. 计算机工程, 2016, 42(9):138-143

[15] Yang Y B, Zhou Y M, Lu H M, et al. Are slice-based cohesion metrics actually useful in effort-aware post-release fault-proneness prediction?: an empirical study[J]. *IEEE Transactions on Software Engineering*, 2014, 41(4): 331-357

[16] Liu X B, Xiao D, Huang W, et al. Quantum block image encryption based on Arnold transform and sine chaotification model[J]. *IEEE Access*, 2019, 7: 57188-57199

[17] Chen L, Sun X Y, Lu M, et al. Contourlet watermarking algorithm based on Arnold scrambling and singular value decomposition [J]. *Journal of Southeast University*, 2012, 28(4): 386-391

[18] Tu S F, Hsu C S. A joint ownership protection scheme for digital images based on visual cryptography[J]. *Interna-*

tional Arab Journal Information Technology, 2012, 9(3): 276-283

[19] Liu F, Wu C K, Lin X J. Colour visual cryptography schemes[J]. *IET Information Security*, 2008, 2(4): 151-165

[20] Su Q T, Yuan Z H, Liu D C. An approximate schur decomposition-based spatial domain color image watermarking method[J]. *IEEE Access*, 2018, 7: 4358-4370

[21] Khalili M, Asatryan D. Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map[J]. *IET Signal Processing*, 2013, 7(3): 177-187

[22] 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

[23] Roy S, Pal A K. A blind DCT based color watermarking algorithm for embedding multiple watermarks[J]. *AEU-International Journal of Electronics and Communications*, 2017, 72: 149-161

[24] Singh S P, Bhatnagar G. A new robust watermarking system in integer DCT domain[J]. *Journal of Visual Communication and Image Representation*, 2018, 53: 86-101

[25] 郭鹏飞, 冯琳, 孙思宇. 新式灰度图像盲检测数字水印算法[J]. 计算机工程与科学, 2019, 41(1):108-116

[26] 陈青, 卜莹, 李伟. 基于 BSVD 分解和 Radon 变换的 NSCT 域鲁棒水印算法[J]. 包装工程, 2019,40(13): 233-238

[27] Liu S H, Yao H X, Gao W, et al. An image fragile watermark scheme based on chaotic image pattern and pixel-pairs[J]. *Applied Mathematics and Computation*, 2007, 185(2): 869-882

[28] 李赵红, 侯建军. 基于 Logistic 混沌映射的 DCT 脆弱数字水印算法[J]. 电子学报, 2006, 34(12):2134-2137

[29] Rawat S, Raman B. A chaotic system based fragile watermarking scheme for image tamper detection[J]. *AEU-International Journal of Electronics and Communications*, 2011, 65(10): 840-847

[30] Azeroual A, Afdel K. Real-time image tamper localization based on fragile watermarking and Faber-Schauder wavelet [J]. *AEU-International Journal of Electronics and Communications*, 2017, 79:207-218

[31] Zhang H, Wang C Y, Zhou X. Fragile watermarking for image authentication using the characteristic of SVD[J]. *Algorithms*, 2017, 10(1): 1382-1396

[32] 侯翔, 闵连权, 杨辉. 利用地理坐标网分块的矢量地图脆弱水印方案[J]. 计算机辅助设计与图形学学报, 2018, 30(11):67-73

[33] 张力, 萧嘉慰, 罗静云. 基于离散小波变换和奇异值分解的盲水印算法[J]. 计算机应用, 2013, 33(s2): 150-152

[34] Thanki R, Kothari A, Trivedi D. Hybrid and blind watermarking scheme in DCuT-RDWT domain[J]. *Journal of Information Security and Applications*, 2019, 46: 231-249

[35] Naik K, Trivedy S, Pal A K. An IWT based blind and robust image watermarking scheme using secret key matrix [J]. *Multimedia Tools and Applications*, 2018, 77(11): 13721-13752

[36] 陈青, 翁旭峰. 一种新的基于伪 Zernike 矩的图像盲水印算法[J]. 计算机应用研究, 2016, 33(9):2810-2818

[37] Kang X B, Zhao F, Lin G F, et al. A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength[J]. *Multimedia Tools and Applications*, 2018, 77(11): 13197-13224

[38] Liu Z, Cui L H. A zero-watermark scheme for identification photos based on QR code and visual cryptography [J]. *International Journal of Security and Its Applications*, 2016, 10(1): 203-214

[39] 刘晶, 王映辉, 刘刚, 等. 一种可抵抗几何攻击的 Directionlet 变换域盲水印算法[J]. 电子与信息学报, 2011, 33(2):442-447

[40] Ye X Y, Chen X T, Deng M, et al. A SIFT-based DWT-SVD blind watermark method against geometrical attacks [C]//2014 7th International Congress on Image and Signal Processing, Dalian, China, 2014: 323-329

[41] Su Q T, Niu Y G, Liu X L, et al. A blind dual color images watermarking based on IWT and state coding[J]. *Optics Communications*, 2012, 285(7): 1717-1724

[42] Su Q T, Niu Y G, Zou H L, et al. A blind dual color images watermarking based on singular value decomposition [J]. *Applied Mathematics and Computation*, 2013, 219(16): 8455-8466

[43] 刘凡, 杨洪勇, 苏庆堂. 基于矩阵 Schur 分解的彩色图像盲水印算法[J]. 计算机应用研究, 2017, 34(10):3085-3089, 3093

[44] 王晓红, 孙业强. 基于 QR 分解的强鲁棒性双彩色盲水印算法[J]. 光电子·激光, 2017, 28(9):88-96

[45] 王晓红, 孙业强. 基于 QR 码和 Schur 分解的双彩色

盲水印算法[J]. 光学技术, 2018,44(1):106-112
[46] 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
[47] Vellaisamy S, Ramesh V. Inversion attack resilient zero-watermarking scheme for medical image authentication [J]. *IET Image Processing*, 2014, 8(12): 718-727
[48] Ali Z, Imran M, Alsulaiman M, et al. A zero-watermarking algorithm for privacy protection in biomedical signals [J]. *Future Generation Computer Systems*, 2018, 82: 290-303
[49] Rani A, Bhullar A K, Dangwal D, et al. A zero-watermarking scheme using discrete wavelet transform [J]. *Procedia Computer Science*, 2015, 70: 603-609
[50] Lang F N, Zhou J J, Cang S, et al. A self-adaptive image normalization and quaternion PCA based color image watermarking algorithm[J]. *Expert Systems with Applications*, 2012, 39(15): 12046-12060
[51] Prathap I, Natarajan V, Anitha R. Hybrid robust watermarking for color images [J]. *Computers and Electrical Engineering*, 2014, 40(3): 920-930
[52] 曲长波, 杨晓陶, 袁铎宁. 小波域视觉密码零水印算法[J]. 中国图象图形学报, 2014, 19(3):365-372
[53] 曲长波, 吴德阳. 基于 Curvelet-DSVD 和视觉密码的强鲁棒零水印算法[J]. 计算机应用研究, 2019, 36(2):218-223
[54] 廖琪男. 基于空域的水印图像几何校正和零水印算法[J]. 计算机工程与应用, 2011, 47(13): 91-94
[55] 熊祥光. 空域彩色图像鲁棒零水印算法[J]. 计算机工程与科学, 2017, 39(1):103-110
[56] 熊祥光. 空域强鲁棒零水印方案[J]. 自动化学报, 2018, 44(1): 160-175
[57] ElGamal A F, Mosa N A, ElSaid W K. Block-based watermarking for color images using DCT and DWT[J]. *International Journal of Computer Applications*, 2013, 66(15): 33-40
[58] Lu W, Sun W, Lu H T. Novel robust image watermarking based on subsampling and DWT [J]. *Multimedia Tools and Applications*, 2012, 60(1): 31-46
[59] Cao H, Zhu G, Zhao H, et al. Novel digital watermarking method based on DWT and DCT[C]// Optical Science and Technology, SPIE's 48th Annual Meeting, San Diego, USA, 2004: 179-187
[60] Yu H Y, Fan J L, Zhang X L. A robust watermark algorithm based on ridgelet transform and fuzzy c-means[C]//2009 International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 2009: 120-124
[61] 曲长波, 于智龙, 李栋栋. 基于分块 FRIT-SVD 的鲁棒零水印算法[J]. 计算机工程与科学, 2018, 40(6):53-64
[62] 石慧, 林闯, 李明楚, 等. 基于 Contourlet 变换的抗几何攻击数字水印算法[J]. 光电子·激光, 2011,22(10):1575-1581
[63] Bazargani M, Ebrahimi H, Dianat R. Digital image watermarking in wavelet, contourlet and curvelet domains [J]. *Journal of Basic and Applied Scientific Research*, 2012, 2(11): 11296-11308
[64] 鲁荣波, 陈留洋, 丁雷, 等. 基于 Contourlet 域虚拟树结构和 FOA-SVR 的自适应鲁棒数字水印算法[J]. 电子学报, 2017,45(3):674-679
[65] Du T S, Ke X T, Liao J G, et al. DSLC-FOA: improved fruit fly optimization algorithm for application to structural engineering design optimization problems [J]. *Applied Mathematical Modelling*, 2018, 55: 314-339
[66] Lu S J, Chen T, Tian S X, et al. Scene text extraction based on edges and support vector regression[J]. *International Journal on Document Analysis and Recognition (IJDAR)*, 2015, 18(2):125-135
[67] Niu Y, Du J Y, Li L L. Digital watermarking system design and implementation based on LSB algorithm[J]. *Key Engineering Materials*, 2010, 439(1): 652-657
[68] Zhang N N. Watermarking algorithm of spatial domain image based on SVD[C]//2016 International Conference on Audio, Language and Image Processing, Shanghai, China, 2016: 361-365
[69] 曲长波, 吴德阳, 肖成龙, 等. RGB 空间彩色零水印算法[J]. 计算机科学与探索, 2019, 13(4): 666-680
[70] 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
[71] Mala S P, Devappa J, Kaliyamoorthy E. Application of fractional wave packet transform for robust watermarking of mammograms [J]. *International Journal of Telemedicine and Applications*, 2015, 2015:1-8
[72] Thakkar F N, Srivastava V K. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications [J]. *Multimedia Tools and Applications*, 2017, 76(3):1-29
[73] Jiang L, Xu Z Q, Xu Y Y. A new comprehensive security protection for remote sensing image based on the integration of encryption and watermarking[C]//2013 IEEE In-

ternational Geoscience and Remote Sensing Symposium, Melbourne, Australia, 2013: 2577-2580

[74] Li D S, Che X Y, Luo W, et al. Digital watermarking scheme for colour remote sensing image based on quaternion wavelet transform and tensor decomposition [J]. *Mathematical Methods in the Applied Sciences*, 2019, 42 (14): 4664-4678

[75] Tong D Y, Ren N, Zhu C Q. Secure and robust watermarking algorithm for remote sensing images based on compressive sensing [J]. *Multimedia Tools and Applications*, 2019, 78(12): 16053-16076

Survey of digital image watermarking technology

Wu Deyang*, Zhang Jinyu***, Rong Wuyan**, Tang Yong*, Zhao Jing*, Qu Changbo***

(*College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004)

(**Ruikang Hospital Affiliated to Guangxi University of Chinese Medicine, Nanning 530011)

(***College of Software, Liaoning Technical University, Huludao 125105)

Abstract

With the rapid development of digital information technology, digital image information is widely used in communication and information representation, but such information is often subject to illegal tampering. Therefore, how to ensure that the copyright of digital images isn't destroyed is a problem that has been faced in the field of digital information. As a copyright protection technology, digital watermark can solve the problem of copyright disputes of images to a certain extent. For this reason, the research on digital image technology is of great significance. This paper systematically summarizes the achievements made by scholars at home and abroad in this research field in recent years. First, the basic model, basic characteristics and measurement indicators of image watermarking are given. Then, the characteristics of existing image watermarking algorithms are analyzed. This paper classifies and introduces the application of watermarking technology in other fields. Next, based on the resistance behavior of watermarking algorithms, it summarizes the robust attacks that can be effectively resisted by existing watermarking algorithms. Finally, according to the advantages and disadvantages of existing watermarking techniques, future development trends and the direction that can be studied next are proposed.

Key words: digital watermarking overview, copyright protection, robustness, blind watermark, zero watermark